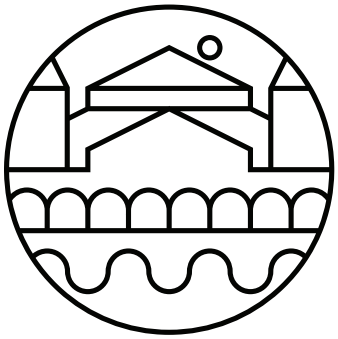
XXXV
SIMPÓSIO BRASILEIRO DE
REDES DE COMPUTADORES
E SISTEMAS DISTRIBUÍDOS

15 a 19 de maio de 2017
Belém - Pará

Anais XIII WP2P+ 2017



XXXV
SIMPÓSIO BRASILEIRO DE
REDES DE COMPUTADORES
E SISTEMAS DISTRIBUÍDOS

15 a 19 de maio de 2017
Belém - Pará

Anais do XIII WP2P+ 2017
Workshop de Redes P2P, Dinâmicas, Sociais e Orientadas a Conteúdo

Editora
Sociedade Brasileira de Computação (SBC)

Organização
Jéferson Campos Nobre (UNISINOS)
Leobino Nascimento Sampaio (UFBA)
Ronaldo Alves Ferreira (UFMS)
Antônio Jorge Gomes Abelém (UFPA)
Eduardo Coelho Cerqueira (UFPA)

Realização
Sociedade Brasileira de Computação (SBC)
Universidade Federal do Pará (UFPA)
Laboratório Nacional de Redes de Computadores (LARC)

Capa: Catarina Nefertari (PCT-UFPA)
Produção Editorial: Denis Lima do Rosário (UFPA)

Cópias Adicionais:
Sociedade Brasileira de Computação (SBC)
Av. Bento Gonçalves, 9500- Setor 4 - Prédio 43.412 - Sala 219
Bairro Agronomia - CEP 91.509-900 - Porto Alegre - RS
Fone: (51) 3308-6835
E-mail: sbc@sbc.org.br

XIII Workshop de Redes P2P, Dinâmicas, Sociais e Orientadas a Conteúdo (13: 2017: Belém, Pa).

Anais / XIII Workshop de Redes P2P, Dinâmicas, Sociais e Orientadas a Conteúdo – WP2P+; organizado por Antônio Jorge Gomes Abelém, Eduardo Coelho Cerqueira, Ronaldo Alves Ferreira, Jéferson Campos Nobre, Leobino Nascimento Sampaio - Porto Alegre: SBC, 2017

74 p. il. 21 cm.
Vários autores
Inclui bibliografias

1. Redes de Computadores. 2. Sistemas Distribuídos. I. Abelém, Antônio Jorge Gomes II. Cerqueira, Eduardo Coelho III. Ferreira, Ronaldo Alves IV. Nobre, Jéferson Campos V. Sampaio, Leobino Nascimento VI. Título.

Sociedade Brasileira da Computação

Contato
Av. Bento Gonçalves, 9500
Setor 4 - Prédio 43.412 - Sala 219
Bairro Agronomia
91.509-900 – Porto Alegre RS
CNPJ: 29.532.264/0001-78
http://www.sbrc.org.br

Laboratório Nacional de Redes de Computadores (LARC)

Diretora do Conselho Técnico-Científico
Rossana Maria de C. Andrade (UFC)

Vice-Diretor do Conselho Técnico-Científico
Ronaldo Alves Ferreira (UFMS)

Diretor Executivo
Paulo André da Silva Gonçalves (UFPE)

Vice-Diretor Executivo
Elias P. Duarte Jr. (UFPR)

Membros Institucionais
SESU/MEC, INPE/MCT, UFRGS, UFMG, UFPE, UFCG (ex-UFPB Campus Campina Grande), UFRJ, USP, PUC-Rio, UNICAMP, LNCC, IME, UFSC, UTFPR, UFC, UFF, UFSCar, IFCE (CEFET-CE), UFRN, UFES, UFBA, UNIFACS, UECE, UFPR, UFPA, UFAM, UFABC, PUCPR, UFMS, UnB, PUC-RS, PUCMG, UNIRIO, UFS e UFU.

Contato
Universidade Federal de Pernambuco - UFPE
Centro de Informática - CIn
Av. Jornalista Anibal Fernandes, s/n
Cidade Universitária
50.740-560 - Recife - PE
http://www.larc.org.br

Organização do SBRC 2017

Coordenadores Gerais
Antônio Jorge Gomes Abelém (UFPA)
Eduardo Coelho Cerqueira (UFPA)

Coordenadores do Comitê de Programa
Edmundo Roberto Mauro Madeira (UNICAMP)
Michele Nogueira Lima (UFPR)

Coordenador de Palestras e Tutoriais
Edmundo Souza e Silva (UFRJ)

Coordenador de Painéis e Debates
Luciano Paschoal Gaspary (UFRGS)

Coordenadores de Minicursos
Heitor Soares Ramos (UFAL)
Stênio Flávio de Lacerda Fernandes (UFPE)

Coordenadora de Workshops
Ronaldo Alves Ferreira (UFMS)

Coordenador do Salão de Ferramentas
Fabio Luciano Verdi (UFSCar)

Comitê de Organização Local
Adailton Lima (UFPA)
Alessandra Natasha (CESUPA)
Davis Oliveria (SERPRO)
Denis Rosário (UFPA)
Elisangela Aguiar (SERPRO)
João Santana (UFRA)
Josivaldo Araújo (UFPA)
Marcos Seruffo (UFPA)
Paulo Henrique Bezerra (IFPA)
Rômulo Pinheiro (UNAMA)
Ronedo Ferreira (META)
Thiêgo Nunes (IFPA)
Vagner Nascimento (UNAMA)

Comite Consultivo
Allan Edgard Silva Freitas (IFBA)
Antonio Alfredo Ferreira Loureiro (UFMG)
Christian Esteve Rothenberg (UNICAMP)
Fabíola Gonçalves Pereira Greve (UFBA)
Frank Augusto Siqueira (UFSC)
Jussara Marques de Almeida (UFMG)
Magnos Martinello (UFES)
Antonio Marinho Pilla Barcellos (UFRGS)
Moisés Renato Nunes Ribeiro (UFES)
Rossana Maria de Castro Andrade (UFC)

Mensagem dos Coordenadores Gerais

Sejam bem-vindos ao 35o Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2017) e a acolhedora cidade das mangueiras - Belém / Pará.

Organizar uma edição do SBRC pela segunda vez no Norte do Brasil é um desafio e um privilégio por poder contribuir com a comunidade de Redes de Computadores e Sistemas Distribuídos do Brasil e do exterior. O SBRC se destaca como um importante celeiro para a discussão, troca de conhecimento e apresentação de trabalhos científicos de qualidade.

A programação do SBRC 2017 está diversificada e discute temas relevantes no cenário nacional e internacional. A contribuição da comunidade científica brasileira foi de fundamental importância para manter a qualidade técnica dos trabalhos e fortalecer a ciência, tecnologia e inovação no Brasil.

Após um cuidadoso processo de avaliação, foram selecionados 77 artigos completos organizados em 26 sessões técnicas e 10 ferramentas para apresentação durante o Salão de Ferramentas. Além disso, o evento contou com 3 palestras e 3 tutoriais proferidos por pesquisadores internacionalmente renomados, 3 painéis de discussões e debates, todos sobre temas super atuais, 6 minicursos envolvendo Big Data, sistemas de transportes inteligentes, rádios definidos por software, fiscalização e neutralidade da rede, mecanismos de autenticação e autorização para nuvens computacionais e comunicação por luz visível, bem como 10 workshops.

O prêmio “Destaque da SBRC” e uma série de homenagens foram prestadas para personalidades que contribuíram e contribuem com a área. O apoio incondicional da SBC, do LARC, do Comitê Consultivo da SBRC e da Comissão Especial de Redes de Computadores e Sistemas Distribuídos da SBC foram determinantes para o sucesso do evento. A realização do evento também contou com o importante apoio do Comitê Gestor da Internet no Brasil (CGI.br), do CNPq, da CAPES, do Parque de Ciência e Tecnologia Guamá, da Connecta Networking, da Dantec Telecom, da RNP e do Google. Nosso especial agradecimento à Universidade Federal do Pará (UFPA) e ao Instituto Federal do Pará (IFPA) pelo indispensável suporte à realização do evento.

Nosso agradecimento também para os competentes e incansáveis coordenadores do comitê do programa (Michele Nogueira/UFRP – Edmundo Madeira/UNICAMP), aos coordenadores dos minicursos (Stênio Fernandes/UFPE – Heitor Ramos/UFAL), ao coordenador dos workshops (Ronaldo Ferreira/UFMS), ao coordenador de painéis e debates (Luciano Gaspary/UFRGS), ao coordenador do Salão de Ferramentas (Fabio Verdi/UFSCar) e ao coordenador de palestras e tutoriais (Edmundo Souza e Silva/UFRJ). Destacamos o excelente trabalho do comitê de organização local coordenado por Denis do Rosário.

Por fim, desejamos a todos uma produtiva semana em Belém.

Antônio Abelém e Eduardo Cerqueira

Coordenadores Gerais do SBRC 2017

Mensagem do Coordenador de Workshops

É com grande prazer que os convido a prestigiar os workshops do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) nos dias 15, 16 e 19 de maio de 2017. Tradicionalmente, os workshops abrem e fecham a semana do SBRC e são responsáveis por atrair uma parcela expressiva de participantes para o Simpósio. Como coordenador de workshops, dividi com os coordenadores gerais do SBRC a nobre tarefa de selecionar os workshops que melhor representam a comunidade e que fortaleçam novas linhas de pesquisa ou mantenham em evidência linhas de pesquisa tradicionais.

Em resposta à chamada aberta de workshops, recebemos dez propostas de alta qualidade, das quais nove foram selecionadas. Além disso, mantivemos a longa colaboração com a RNP por meio da organização do WRNP, que já é uma tradição na segunda e terça-feira da semana do SBRC. Dentre as propostas aceitas, sete são reedições de workshops tradicionais do SBRC que já são considerados parte do circuito nacional de divulgação científica nas várias subáreas de Redes de Computadores e Sistemas Distribuídos, como o WGRS (Workshop de Gerência e Operação de Redes e Serviços), o WTF (Workshop de Testes e Tolerância a Falhas), o WCGA (Workshop em Clouds, Grids e Aplicações), o WP2P+ (Workshop de Redes P2P, Dinâmicas, Sociais e Orientadas a Conteúdo), o WPEIF (Workshop de Pesquisa Experimental da Internet do Futuro), o WoSiDA (Workshop de Sistemas Distribuídos Autonômicos) e o WoCCES (Workshop de Comunicação de Sistemas Embarcados Críticos). Como novidade, teremos dois novos workshops com programação diversificada e grande apelo social, o CoUrb (Workshop de Computação Urbana) e o WTICp/D (Workshop de TIC para Desenvolvimento).

Temos certeza que 2017 será mais um ano de sucesso para os workshops do SBRC pelo importante papel de agregação que eles exercem na comunidade científica de Redes de Computadores e Sistemas Distribuídos no Brasil.

Aproveitamos para agradecer o apoio recebido de diversos membros da comunidade e, em particular, a cada coordenador de workshop, pelo brilhante trabalho. Como coordenador dos workshops, agradeço imensamente o apoio recebido da Organização Geral do SBRC 2017.

Esperamos que vocês aproveitem não somente os workshops, mas também todo o SBRC e as inúmeras atrações de Belém.

Ronaldo Alves Ferreira

Coordenador de Workshops do SBRC 2017

Mensagem dos Coordenadores do XIII WP2P+ 2017

O Workshop de Redes P2P, Dinâmicas, Sociais e Orientadas a Conteúdo (WP2P+) é um fórum para a discussão do estado da arte e dos atuais desafios de pesquisa em teoria, tecnologias e aplicações de redes colaborativas e dinâmicas. O público do WP2P+ é formado por usuários interessados na geração e disseminação de informações com suporte de conceitos relativos aos sistemas P2P, dinâmicos, redes sociais, redes de cache ou orientados a conteúdo. Em sua décima-terceira edição em 2017, o workshop tem se consolidado como um importante espaço para a apresentação de resultados e trocas de experiências da comunidade brasileira da área.

No WP2P+, cada artigo recebeu três revisões de membros do comitê de programa ou de revisores tutelados por estes. Ao fim do processo, com o objetivo de maximizar as oportunidades de discussão e assim fortalecer a área, 7 artigos foram selecionados para apresentação no workshop. A seleção dos artigos é composta de uma diversidade significativa de tópicos e certamente proporcionará à comunidade bastante material para discussões produtivas.

A fim de atrair um maior interesse da comunidade, assim como, oferecer um novo espaço para discussão sobre os temas ligados ao workshop, a edição de 2017 do Wp2p+ contará com a participação de Daniel Sadoc Menasche como palestrante. Além disso, foram incluídos novos membros ao comitê de programa.

O mérito do WP2P+ é resultante dos esforços dos autores dos artigos submetidos, dos membros do comitê de programa e do comitê de organização do SBRC 2017, na pessoa de Antônio Abelém e Eduardo Cerqueira, como coordenadores gerais, e Ronaldo Ferreira, como coordenador dos workshops. Agradecemos o apoio e a confiança de todos na realização do WP2P+ 2017.

Um bom workshop a todos.

Jéferson Campos Nobre, Leobino Nascimento Sampaio

Coordenadores do WP2P+ 2017

Comitê de Programa

- Alex Borges Vieira (UFJF)
- Ana Paula Couto e Silva (UFMG)
- Antônio Augusto de Aragão Rocha (UFF)
- Artur Ziviani (LNCC)
- Carlos Kamienski (UFABC)
- Christian Esteve Rothemberg (UNICAMP)
- Daniel Figueiredo (UFRJ)
- Daniel Sadoc Menasche (UFRJ)
- Fábio Luciano Verdi (UFSCar)
- Humberto Marques (PUC Minas)
- Ítalo Cunha (UFMG)
- Jéferson Campos Nobre (UNISINOS)
- Jussara Almeida (UFMG)
- Lásaro Jonas Camargo (UFU)
- Leobino Nascimento Sampaio (UFBA)
- Lisandro Z. Granville (UFRGS)
- Luciano Bernardes de Paula (IFSP)
- Luis Carlos de Bona (UFPR)
- Magnos Martinello (UFES)
- Michele Nogueira (UFPR)
- Rafael Pasquini (UFU)
- Rodolfo da Silva Villaça (UFES)
- Sidney Lucena (UNIRIO)
- Weverton Cordeiro (UFRGS)

Sumário

XIII Workshop de Redes P2P, Dinâmicas, Sociais e orientadas a Conteúdo (WP2P+)

SBRC 2017

Sessão Técnica 1 – Artigos Curtos

Redes Veiculares: Uma proposta de aplicação para veículos de resgate

Lauro de Lacerda Caetano, Arthur Albuquerque Zopellaro Soares, Vinicius Barcelos da Silva

Instituto Federal de Educação, Ciência e Tecnologia Fluminense – Campos dos Goytacazes, RJ – Brasil

{laurodelacerda,arthurazsoares}@gmail.com, viniciusbs@iff.edu.br

Resumo. *Neste trabalho, é proposta uma aplicação p2p para redes veiculares focada na disseminação de dados de localização de veículos de resgate. A aplicação desenvolvida utiliza dados de posicionamento atuais e futuros destes veículos para enviar pacotes broadcast, solicitando que os veículos próximos abram passagem. Com base nos resultados obtidos a partir de experimentos de simulação, foram comparados os tempos de percurso e velocidade do veículo de resgate em um cenário base com outro cenário onde a aplicação é utilizada. Os resultados mostraram um tempo menor de percurso quando a aplicação proposta é ativada nos veículos.*

1. Introdução

Nas grandes cidades, uma das questões intensamente debatidas é o trânsito e as possíveis alternativas para diminuição do volume de veículos. Quando se trata de trânsito, é inquestionável a sua influência no atraso de atendimentos de resgate ou emergência, mesmo havendo a utilização de sirenes e giroscópios por parte de ambulâncias ou carros do corpo de bombeiros.

Nos últimos anos, as redes *ad hoc* veiculares (VANETs - *Vehicular Ad Hoc Networks*) surgiram como relevante tecnologia de apoio na gestão inteligente de cidades, podendo atuar para a melhoria da eficiência e da segurança dos sistemas de transporte [Vegni, Biagi & Cusani 2013].

Neste trabalho, é proposta uma aplicação para auxiliar veículos de resgate na abertura de passagem no trânsito, com o objetivo de reduzir o tempo de trajeto destes veículos. Resgates mais rápidos a possíveis vítimas seriam o benefício direto oferecido por esta aplicação.

2. Metodologia

Para desenvolvimento da aplicação e simulação dos cenários é preciso utilizar softwares que compartilhem de forma bidirecional informações de rede e de mobilidade. Estes dados são gerados respectivamente por um (1) software de simulação de redes e um (2) software de simulação de tráfego multimodal.

O software simulador de redes escolhido é o OMNET++ 5.0 [OpenSim 2003]. Este atuará como plataforma de desenvolvimento da aplicação. O *framework* Veins 4.4

[Sommer 2014], que dispõe de uma biblioteca de redes veiculares, servirá como o *middleware* de comunicação bidirecional utilizando uma interface de controle de tráfego chamada TraCI [Wegener et al. 2008]. E para simular os cenários de tráfego multimodal, o software SUMO 0.25 será utilizado.

3. Aplicação para veículos de resgate

A fim de alcançar o objetivo deste trabalho, o código fonte do Veins foi utilizado como base, e uma aplicação foi desenvolvida. Esta aplicação, quando ativada, envia mensagens periódicas aos dispositivos sem-fio nas redondezas. A partir do recebimento destas mensagens, os nós (veículos comuns) podem ser orientados para uma melhor tomada de decisão no trânsito. Um diagrama de classes simplificado da aplicação desenvolvida é apresentado na Figura 1. As classes que a compõem interagem com classes já existentes no pacote do *framework* Veins. Maiores informações sobre as classes podem ser vistas em [Caetano & Soares 2016].

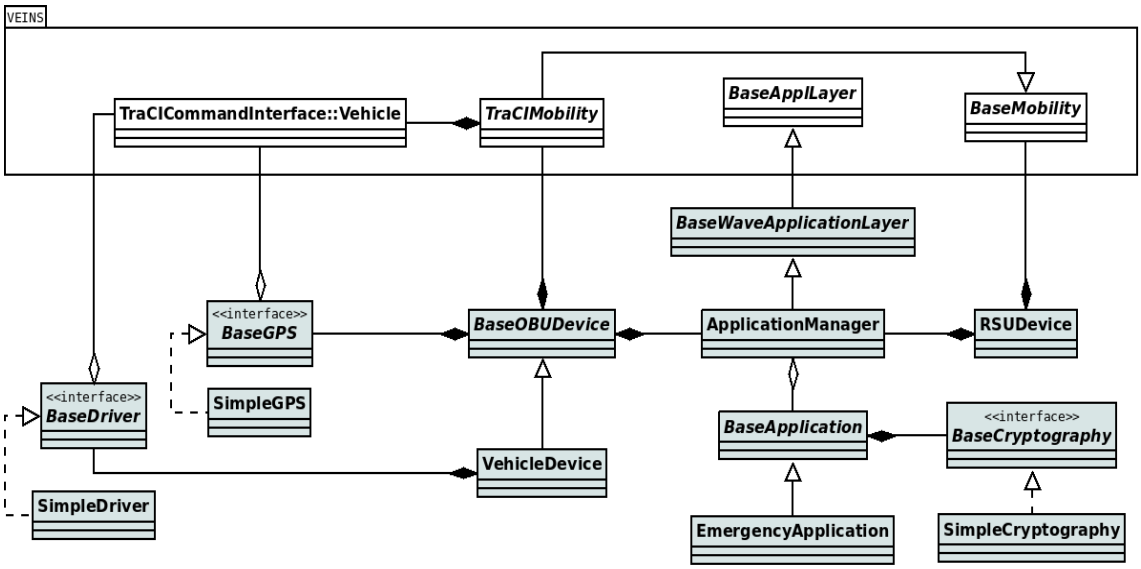


Figura 1. Diagrama de Classes do código desenvolvido

A classe ***EmergencyApplication*** (Algoritmo 1) gera os dados da aplicação que são posteriormente transformados em mensagens e encapsulados em cabeçalhos por camadas inferiores. As mensagens criadas na camada de aplicação de redes veiculares são também chamadas de mensagens de serviço WAVE (WSM – WAVE Short Message) [IEEE 1609.3 2016].

As WSMs são criadas pela aplicação a partir de uma WSM base para envio dos dados. Estas mensagens são do tipo broadcast com único salto (*single-hop*). Os campos seguintes são adicionados ao cabeçalho da WSM:

- Identificação de Provedor de Serviço: Campo hexadecimal, também chamado de PSID (*Provider Service Identifier*), que contém a natureza da mensagem [IEEE 1609.3 2016]. Nesta aplicação a mensagem será do tipo "Aviso de Emergência" tendo o código hexadecimal 0x0C [IEEE 1609.12 2016].
- Número do Canal de Rádio: Informa o canal de rádio utilizado para transmissão

das mensagens.

- Comprimento dos Dados.
- Dados da Mensagem.

```
1  std::string dados = gps->obterRota(numeroDeRuas);
2  std::string dadosEncriptados = criptografia->encriptar(dados);
3
4  WaveShortMessage* wsm = new WaveShortMessage(*wsmBase);
5  wsm->adicionarDado(dadosEncriptados);
6  wsm->adicionarPsid(0x0C);
7  wsm->adicionarCanal(Canais::CCH);
8  wsm->adicionarComprimentoDaMensagem(dadosEncriptados.size());
9
10 return wsm;
```

Algoritmo 1. Parte de código contido na classe *EmergencyApplication*

O campo de dados recebe as coordenadas do veículo de resgate, que são obtidas do SUMO por meio da interface TraCI. Com isso, assume-se que cada veículo, inclusive o de resgate, possui um GPS e conhece sua rota. Na aplicação desenvolvida há uma variável (parâmetro **numeroDeRuas** em Algoritmo 1) que estabelece o número máximo de ruas a serem enviadas na mensagem de *broadcast*. As coordenadas obtidas são organizadas da seguinte forma dentro do campo de dados:

$$(L_1)[R_1][R_2] \ldots [R_n]$$

L_1 e R_1 representam respectivamente a faixa e o trecho em que o veículo está transitando. R_2 até R_n indicam os próximos trechos a serem percorridos. O número n assume o valor estabelecido na variável **numeroDeRuas** (Algoritmo 1), sendo necessário um valor mínimo de 1 rua. O valor deste parâmetro pode ser escalado a fim de se produzir novos estudos.

O código desenvolvido também trata do comportamento da camada de aplicação ao receber WSMs. A partir do recebimento destas, confere-se o PSID no cabeçalho da mensagem a fim de encaminhar o pacote para descarte ou tratamento cabível. Caso o PSID seja o hexadecimal 0x0C, a aplicação de resgate tratará a mensagem recebida. A aplicação orientará o nó receptor a uma mudança de faixa caso o mesmo esteja em rota de colisão com o nó emissor. A classe ***SimpleDriver*** (Figura 1), que representa os comportamento de um condutor, realizará a mudança de faixa quando possível.

Veículos comuns que estão em ruas paralelas ao veículo de emergência, ou seja, fora de sua rota de colisão, também recebem a mensagem devido a sua natureza (*broadcast*), entretanto, após analisar a rota contida na mensagem recebida, descartam a mensagem, visto que estão em percursos diferentes em relação ao veículo de resgate.

4. Estudo de Caso

Para criação de um estudo de caso, foi escolhida uma região na cidade do Rio de Janeiro

para ser o cenário do experimento que simula o funcionamento da aplicação desenvolvida. Foi exportado um mapa das regiões de Ipanema e Copacabana utilizando a ferramenta aberta OpenStreetMaps.

O percurso do veículo de resgate é mostrado em vermelho na Figura 2. Este percurso poderia representar, em um ambiente real, a configuração da rota realizada pelo motorista do veículo de resgate em um aplicativo de GPS.

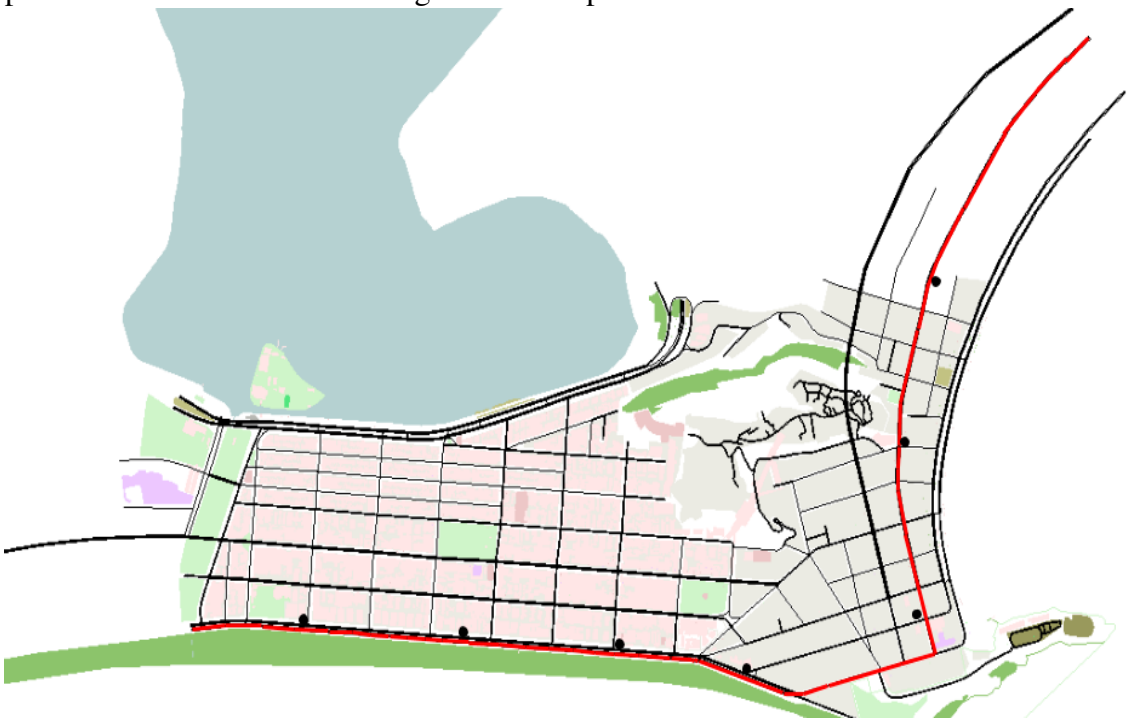


Figura 2. Trajeto do veículo de resgate em cenário real

Um número de veículos comuns foram dispersos pelo percurso baseando-se em informações sobre o volume de tráfego apresentados pela Companhia de Engenharia de Tráfego do Rio de Janeiro [CET-Rio 2014]. Todos os veículos portam rádios de comunicação 802.11p e foram programados para atuarem como receptores de mensagens da aplicação desenvolvida, salvo o veículo de resgate que irá exercer o papel de transmissor.

Tabela 1. Configuração dos rádios IEEE 802.11p

Parâmetro	**Valor**
Potência de Transmissão	200mW
Limite de atenuação de sinal	-89dBm
Frequência	5.89 GHz
Ruído Térmico	-110dBm
Sensibilidade da camada física	-89dBm
Alcance do rádio	1000m

Simulações preliminares foram realizadas com o objetivo de indicar valores

ótimos de periodicidade do envio de mensagens e de número de ruas para a aplicação de resgate no trecho em questão. Tais valores foram atribuídos às variáveis no estudo de caso.

Tabela 2. Configurações da aplicação de resgate

Parâmetro	**Valor**
Periodicidade de envio	0.5s
numeroDeRuas	4

Também foram espalhados no cenário rádios de comunicação estáticos, chamados de RSUs, que são unidades de acostamento que replicam a mensagem baseando-se na informação do PSID da mesma. A replicação aumenta o alcance das mensagens permitindo que um maior número de veículos receba o aviso. A classe ***EmergencyApplication*** (Figura 1) gerencia uma lista contendo as últimas mensagens replicadas, de forma a reenviar a mesma mensagem apenas uma vez. Esta medida ajuda a conter a inundação de difusões (*broadcast storms*).

Conceitualmente, seria possível dizer que os veículos comuns que receberem a mensagem de emergência poderiam representar as informações recebidas através de uma interface multimídia/computador de bordo e emitir alertas sonoros em uma situação real. Estes alertas poderiam requisitar uma ação do motorista para desobstruir a passagem do veículo de resgate caso este esteja nos arredores.

5. Análise dos Resultados

O desempenho da aplicação é medido ao comparar sua influência no tempo de percurso e na velocidade média do veículo de resgate com um cenário base, o qual não há uso da aplicação.

Em ambos os cenários, 100 simulações foram realizadas fazendo uso de um mesmo conjunto de sementes aleatórias. As sementes são geradas através do algoritmo *Mersenne Twister* do SUMO [Krajzewicz et al. 2012].

Após a simulação, foram coletados os dados e removidos os valores atípicos (também chamados de *outliers*) do conjunto, o que produz uma análise com confiabilidade de 95%.

Tabela 3. Resultados

Resultados	**Sem Aplicação**	**Com Aplicação**
Total Percorrido	4800m	4800m
Tempo médio	471,53s	452,25s
Velocidade média	36,65 km/h	38,21 km/h

A partir dos dados gerados, verificamos que a economia de tempo foi de 19,28

segundos em relação ao cenário sem utilização da aplicação. Também é possível notar um aumento na velocidade média do veículo de resgate.

6. Conclusão e Trabalhos Futuros

Neste trabalho, foi apresentada uma aplicação desenvolvida para redes veiculares direcionada a veículos de resgate. Os resultados mostraram que redes veiculares podem ser uma alternativa para melhoria do fluxo de veículos de resgate no trânsito, aliados a outros instrumentos como giroscópio e sirenes. Os resultados das simulações mostraram que a utilização da aplicação trouxe um menor tempo de percurso para os veículos de resgate. Como trabalhos futuros, pretende-se investigar o funcionamento desta aplicação de resgate em diferentes condições de tráfego, assim como em combinação com semáforos inteligentes.

Referências

Vegni, A. M.; Biagi, M.; Cusani, R. (2013). “Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks”. In: GIORDANO, L. G. (Ed.); REGGIANI L. (Ed.). Vehicular Technologies - Deployment and Applications. InTech. 19 p.

OpenSim. (2003). "OMNeT: Objective Modular Network Testbed in C++". Disponível em: https://omnetpp.org/omnetpp. Acessado em: 29 de abril de 2017.

Sommer, C. (2014). “Veins”. Disponível em: http://veins.car2x.org/. Acessado em: 09 de abril de 2017.

Wegener, A.; Piorkowski, M.; Raya, M.; Hellbruck, H,; Fischer, S.; Hubaux, J. (2008). “TraCI: An Interface for Coupling Road Traffic and Network Simulators”. Proceedings of the 11th communications and networking simulation symposium. p. 155-163.

Caetano, L. L.; Soares, A. A. Z. (2016). “Redes Veiculares: Tendências e Estudo de Caso”. Disponível em: https://goo.gl/bGjDjY. Acessado em: 09 de abril de 2017.

IEEE Computer Society. (2016) “IEEE Standard for Wireless Access in Vehicular Environments (WAVE): Networking Services”, 1609.3-2016. Nova York. 160 p.

IEEE Computer Society. (2016) “IEEE Standard for Wireless Access in Vehicular Environments (WAVE): Identifier Allocations”, 1609.12-2016. Nova York. 21 p.

CET-RIO. (2014). “Volume Diário De Veículos Das Principais Vias Do Município Do Rio De Janeiro”. Disponível em: http://www.rio.rj.gov.br/dlstatic/10112/5112752/4131653/VolumedasprincipaisviasdoRiodeJaneiro.pdf. Acessado em: 04 de o de 2016.

Krajzewicz, D.; Erdmann, J.; Behrisch, M.; Bieker, L. (2012). “Recent Development and Applications of SUMO – Simulation of Urban MObility”. International Journal on Advances in Systems and Measurements. Disponível em: http://www.sumo.dlr.de/pdf/sysmea_v5_n34_2012_4.pdf. Acessado em: 09 de abril de 2017.

Mobilidade em NDN: Consumidores versus Produtores

Francisco R. C. Araújo[1*], **Leobino N. Sampaio**[1]

[1]Programa de Pós-Graduação em Ciência da Computação (PGCOMP)
Instituto de Matemática – Universidade Federal da Bahia (UFBA)
Salvador – BA – Brasil

{franciscorca, leobino}@ufba.br

Resumo. *As ICNs surgiram para reconstruir uma arquitetura que atenda as demandas, atuais e futuras, da Internet. NDN apresenta-se como uma arquitetura ICN de destaque por possuir diversas características para a Internet do Futuro, sua comunicação baseia-se em consumidores que requisitam interesses aos produtores para a obtenção de dados. A mobilidade do consumidor é razoavelmente suportada pela arquitetura, no entanto, a mobilidade do produtor é um desafio por apresentar danos à rede. Neste contexto, este trabalho apresenta avaliações sobre os diferentes impactos causados na rede pela mobilidade do produtor e do consumidor. Os experimentos realizados evidenciam os desafios de manter a comunicação ativa com o produtor móvel.*

1. Introdução

A quantidade de dispositivos e a forma de acesso à *Internet* mudaram significativamente nos últimos anos. De acordo com a [Cisco 2016], o tráfego de dados móveis global cresceu 74% em 2015 e a perspectiva é que alcance o valor de 30,6 *exabytes* mensais em 2020. No entanto, a arquitetura da *Internet* foi projetada para uma época em que um conjunto limitado de máquinas compartilhavam recursos entre si, o que resultou em um modelo de comunicação entre duas máquinas finais [Jacobson et al. 2009].

Diante das novas demandas em torno da utilização da *Internet* surgiram as *Information-Centric Networking* (ICN). Há várias abordagens em ICN [Xylomenos et al. 2014] [Liu et al. 2017]. Dentre estas abordagens ganharam destaque as *Content Centric Network* (CCN) [Jacobson et al. 2009], bem como sua sucessora *Named Data Networking* (NDN) [Zhang et al. 2014]. CCN/NDN possuem três estruturas: (I) *Forwarding Information Base* (FIB) mantém as rotas para as fontes de dados (produtores); (II) *Pending Interest Table* (PIT) mantém os registros de interesses, que ainda não foram atendidos, para possibilitar que os dados retornem aos solicitantes (consumidores); (III) *Content Store* (CS) armazena os dados em *cache* para atender a futuros interesses.

Em NDN não existe estabelecimento de conexão, os consumidores emitem interesses na rede que responde com os dados solicitados. Esta característica possibilita o suporte a mobilidade do consumidor, pois ao se mover para uma nova rede o consumidor basta enviar novamente os interesses para os dados que ainda não recebeu. Por outro lado, a mobilidade do produtor apresenta um desafio em aberto [Zhang et al. 2016]. Devido às mudanças nos nomes dos conteúdos e ao tempo necessário para atualizar as tabelas de roteamento ao longo da rede [Xylomenos et al. 2014] [Huynh et al. 2017].

[*]Os autores agradecem a Fundação de Amparo à Pesquisa do Estado da Bahia – FAPESB, pelo apoio financeiro.

Este trabalho apresenta a seguinte contribuição: uma análise comparativa entre os danos ocasionados pela mobilidade do produtor e pela mobilidade do consumidor em Redes Centradas no Conteúdo. Além disso, apresenta uma visão geral do estado da arte relacionado a mobilidade de produtores em NDN.

O restante do artigo está organizado da seguinte forma: a Seção 2 apresenta o estado da arte relacionado a mobilidade em NDN. A Seção 3 apresenta a descrição do ambiente adotado nos experimentos. A Seção 4 aborda as avaliações relacionadas aos impactos causados na rede pela mobilidade de nós; e por fim, a Seção 5 conclui o trabalho e discute direções para trabalhos futuros.

2. Estado da Arte

Diversas abordagens surgiram para investigar o problema da mobilidade do produtor em NDN. Dado o fluxo bidirecional de pacotes de interesses/dados, a mobilidade em NDN pode ser dividida em dois sub-problemas: como os dados solicitados podem ser devolvidos a um consumidor em movimento (mobilidade de consumidores); e como os interesses podem atingir os dados gerados pelos produtores em movimento (mobilidade de produtores) [Zhang et al. 2016].

1. **Mobilidade do consumidor** – Quando um consumidor se move em NDN, ele pode simplesmente emitir novas mensagens de interesse a partir de seu local atual para os dados que ainda não recebeu. Se os caminhos antigos e novos se cruzam, os interesses reexpressos recuperam os dados anteriormente solicitados da CS do primeiro roteador comum a ambos os caminhos, ou são combinados com o interesse anterior sem se propagar mais [Zhang et al. 2016]. No entanto, os pacotes de dados correspondentes também serão entregues à sua localização antiga [Xylomenos et al. 2014].
2. **Mobilidade do produtor** – Em NDN, o nome do conteúdo é usado para identificar cada conteúdo e também encapsulado em pacotes NDN para roteamento. A vinculação Localizador/Identificador torna a mobilidade do produtor mais desafiadora. Primeiro, um produtor móvel precisa anunciar os prefixos de nome do conteúdo em um novo local, o que traz grande pressão e grave problema de escalabilidade no plano de roteamento. Em segundo lugar, os interesses dos consumidores de conteúdo podem ir para os antigos locais desatualizados o que causa *timeout* e retransmissão de interesse [Gao and Zhang 2016].
   O apoio à mobilidade de produtores na NDN continua a ser um desafio de investigação em aberto, particularmente no caso de transmissões em tempo real, como vídeo *streaming* [Ge et al. 2016].

De acordo com [Lehmann et al. 2016] a mobilidade dos produtores pode ser dividida em dois períodos: (1) indisponibilidade – caracterizado pela falta de conectividade de rede do produtor durante a mobilidade, e (2) reconexão – refere-se ao processo de restabelecer a conectividade do produtor. Para tratar o período de indisponibilidade do produtor [Lehmann et al. 2016] classifica, de acordo com a literatura, quatro categorias de extensão da arquitetura NDN:

1. **Envio proativo** – Visa manter os dados disponíveis, através de replicação proativa, em vez de manter a alta disponibilidade do produtor. Antes de se deslocar, o produtor descarrega os dados proativamente para o solicitante. O roteador que recebe os dados os armazena, para atender aos pedidos futuros [Lehmann et al. 2016].

2. **Armazenar e encaminhar pedidos** – Tenta evitar a perda de pacotes de interesses e seus reenvios, através da adição de um elemento de rede responsável pelo armazenamento de pedidos em períodos de indisponibilidade do produtor e reencaminhá-los quando o produtor retoma à rede [Lehmann et al. 2016].
3. **Usar a comunicação padrão NDN ou estendê-la** – Algumas abordagens usam a comunicação padrão: mapeamento dos nomes de dados persistentes e temporários de produtores móveis; detecção de degradação no sinal do *link* atual do produtor causado pelo movimento. Outras abordagens estendem o protocolo NDN, através de um esquema que usa âncoras roteáveis para rastrear o movimento do produtor [Lehmann et al. 2016].
4. **Técnicas não NDN para suporte à mobilidade** – Abordagens que fazem uso de técnicas contrárias aos princípios NDN propostos por [Jacobson et al. 2009]. É empregado o uso de outras tecnologias como roteamento guloso, que pode coexistir com o roteamento padrão NDN, combinado com pontos de indireção; SDN combinada com NDN para atualizar as FIBs globais e locais [Lehmann et al. 2016].

3. Cenário

Para realizar os experimentos, foi utilizado o ndnSIM[1] um simulador de ICN baseado no NS-3[2]. O ndnSIM é escrito em C++ e oferece uma plataforma de simulação comum e amigável, além disso, está em sincronia com a equipe de pesquisa NDN, o que resulta em uma combinação da plataforma de simulação com os mais recentes avanços da pesquisa NDN [Mastorakis et al. 2016].

O cenário dos experimentos consiste em seis nós. Dois Pontos de Acesso (APs – AP1 e AP2), dois roteadores (UFBA-rt1 e UFBA-rt2), um nó fixo denominado Nó-A e um nó móvel identificado com o número 5. A Figura 1 representa visualmente a topologia empregada. Foi usado a GUI *visualizer* e a topologia foi descrita em um arquito `.txt`.

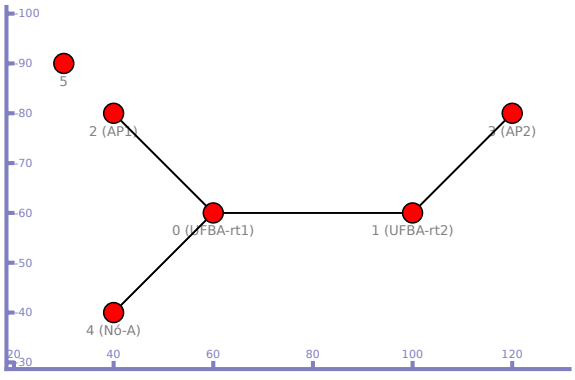
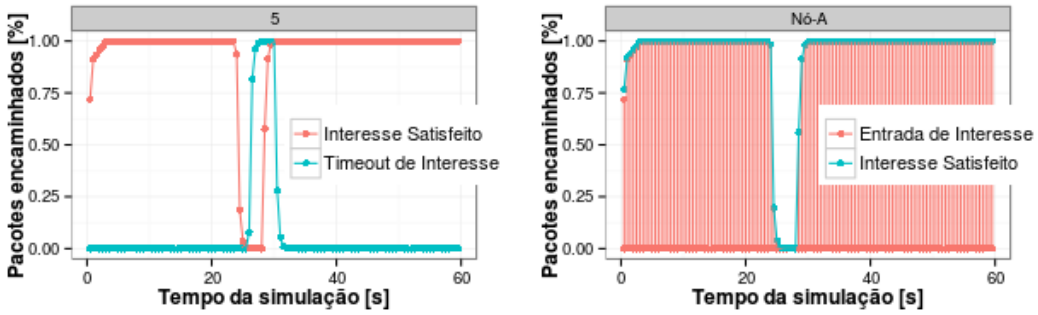


Figura 1. Topologia da rede. Dois tipos de experimentos: (1) Nó 5 é o Consumidor móvel e o Nó-A é o Produtor fixo, e (2) o caso inverso.

O consumidor requisita 100 interesses por segundo a uma frequência constante, para isso, foi utilizado a aplicação *ConsumerCbr* e o produtor irá responder aos interesses recebidos, através da aplicação *Producer*. Foi empregada a estratégia de encaminhamento

[1] `http://ndnsim.net/2.3/`
[2] `https://www.nsnam.org/`



(a) Consumidor Móvel. (b) Produtor Fixo.

Figura 2. Caso 1: Consumidor Móvel e Produtor Fixo

multicast e a política de descarte LRU padrão. O tempo da simulação para cada caso foi de exatamente 60 segundos, tempo suficiente para o nó móvel 5 sair da rede do AP1 e se conectar a rede do AP2, efetuando o *handoff*.

Como o objetivo deste trabalho é evidenciar as diferenças da mobilidade do consumidor e do produtor sobre a NDN, em seu estágio atual, foi adotado apenas os recursos providos pelo simulador, assim, não estendemos suas funcionalidades, para não interferir na arquitetura padrão NDN, isto será feito em trabalhos futuros.

4. Experimentos

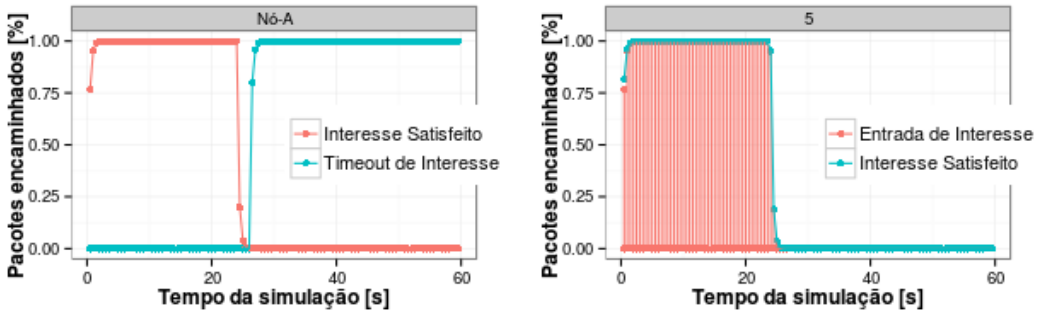
As avaliações realizadas, do impacto da mobilidade de nós em NDN, visam evidenciar através de experimentos as diferenças entre a mobilidade do consumidor e do produtor.

4.1. Impactos da mobilidade do consumidor

Para obter o comportamento do consumidor móvel na rede, foi realizado um experimento com o nó 5 (ver Figura 1) representando o consumidor móvel e o Nó-A representando o produtor fixo. Os impactos da mobilidade do consumidor podem ser observado na Figura 2. Na Figura 2(a) está representado os impactos da mobilidade sobre o consumidor e na Figura 2(b) sobre o produtor.

O consumidor móvel (Nó 5) inicialmente está conectado à rede do AP1 e se move em direção a rede do AP2. A Figura 2(a) mostra que a porcentagem de interesses satisfeitos tem uma queda brusca por volta do tempo 25, essa queda representa exatamente o momento em que o consumidor começa a perder o sinal do AP1 até o momento em que se reconecta à rede no AP2, ou seja, o período do *handoff*. Como reação a não obtenção de dados, nesse período de transição, o *timeout* de interesses se eleva inversamente proporcional à porcentagem de interesses satisfeitos. No entanto, apesar de haver uma queda na comunicação com o consumidor, a arquitetura da rede consegue restabelecê-la, pois logo após o consumidor se conectar ao AP2, reexpressa seus interesses a partir da sua nova rede. Assim, o *timeout* de interesses cai para zero novamente como consequência do restabelecimento da comunicação.

Na Figura 2(b), é possível observar os efeitos sobre o produtor fixo. Este responde a todos os interesses que consegue alcançá-lo. Essa pequena queda na comunicação, representa maiores prejuízos principalmente para aplicações em que atrasos são críticos.



(a) Consumidor Fixo.

(b) Produtor Móvel.

Figura 3. Caso 2: Consumidor Fixo e Produtor Móvel.

4.2. Impactos da mobilidade do produtor

Por outro lado, para obter o comportamento do produtor móvel, foi realizado um experimento com o nó 5 (ver Figura 1) representando o produtor móvel e o Nó-A representando o consumidor fixo. Os impactos da mobilidade do produtor estão representado na Figura 3. A Figura 3(b) retrata as reações da mobilidade no produtor e a Figura 3(a) no consumidor.

O produtor móvel (Nó 5) inicialmente encontra-se na rede do AP1 e se desloca rumo ao AP2. A satisfação de interesses é mantida em sua totalidade até o momento em que produtor perde o sinal com o AP1 (Figura 3(b)). Neste ponto, por volta do tempo 25, a porcentagem de satisfação de interesses se degrada rapidamente atingindo o eixo zero, exatamente no período do *handoff*. O produtor se reconecta na rede do AP2, no entanto, a arquitetura não consegue provê o restabelecimento da comunicação neste caso, pois a comunicação parte do consumidor. Observando a Figura 3(a) nota-se que o consumidor continua a expressar interesses na rede, mas estes atingem constantemente o *timeout* a partir do momento que ocorre o *handoff* do produtor móvel.

Neste experimento, se torna evidente que a arquitetura da rede não dar suporte adequado aos produtores móveis. Assim, nessa direção alguns trabalhos recentes tem investigado mecanismos (como os descritos na Seção 2) para manter a satisfação de interesses elevada mesmo que o produtor seja móvel.

5. Conclusão e Trabalhos Futuros

Diante das novas demandas da *Internet* surgiu a filosofia das ICNs, dentre as várias arquiteturas, a NDN tem ganhado destaque, mas ainda possui alguns problemas que necessitam de investigação, como o caso da mobilidade de nós. No entanto, estas abordagens se mostram de cunho experimental, o que torna difícil a sua reprodução em ambientes reais. Pois estas arquiteturas se diferem da arquitetura atual (TCP/IP) principalmente da camada de rede. Para facilitar pesquisas com essas novas redes pode-se empregar a técnica de simulação.

Nesse contexto, esse trabalho apresentou um breve reflexo do estado da arte relacionado a mobilidade de nós em Redes Centradas no Conteúdo. Um estudo comparativo entre a mobilidade do consumidor e a mobilidade do produtor foi apresentado para evidenciar os diferentes impactos causados na rede. Os resultados dos experimentos tornam

explícito a divergência nas formas com que a arquitetura da rede reage diante da mobilidade do consumidor e do produtor.

Diversas questões teóricas e práticas em ICN em geral e em NDN especificamente necessitam de uma melhor investigação, no entanto, para trabalhos futuros nos atentaremos as questões relacionadas à mobilidade de nós, nesse sentido enumeramos as seguintes:

- Suporte a mobilidade de produtores para aplicações de tempo real;
- Suporte a mobilidade de produtores e consumidores em paralelo.

Referências

Cisco (2016). Cisco Visual Networking Index (VNI) Update Global Mobile Data Traffic Forecast Update, 2015-2020. Technical report, Cisco.

Gao, S. and Zhang, H. (2016). Scalable Mobility Management for Content Sources in Named Data Networking. In *2016 13th IEEE Annual Consumer Communications \& Networking Conference (CCNC)*, pages 79–84.

Ge, J., Wang, S., Wu, Y., Tang, H., and E, Y. (2016). Performance improvement for source mobility in named data networking based on global–local FIB updates. *Peer-to-Peer Networking and Applications*, 9(4):670–680.

Huynh, T., Priyono, O., Lee, S.-H., and Hwang, W.-J. (2017). Simultaneous mobility of data sources and content requesters in content-centric networking. *Peer-to-Peer Networking and Applications*, 10(1):31–44.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., and Braynard, R. L. (2009). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies - CoNEXT '09*, volume 6, pages 1–12. ACM Press.

Lehmann, M. B., Barcellos, M. P., and Mauthe, A. (2016). Providing producer mobility support in NDN through proactive data replication. In *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, pages 383–391. IEEE.

Liu, X., Li, Z., Yang, P., and Dong, Y. (2017). Information-centric mobile ad hoc networks and content routing: A survey. *Ad Hoc Networks*, 58:255–268.

Mastorakis, S., Afanasyev, A., Moiseenko, I., and Zhang, L. (2016). ndnSIM 2: An updated NDN simulator for NS-3. Technical Report NDN-0028, Revision 2, NDN.

Xylomenos, G., Ververidis, C. N., Siris, V. A., Fotiou, N., Tsilopoulos, C., Vasilakos, X., Katsaros, K. V., and Polyzos, G. C. (2014). A Survey of information-centric networking research. *IEEE Communications Surveys and Tutorials*, 16(2):1024–1049.

Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., claffy, k., Crowley, P., Papadopoulos, C., Wang, L., and Zhang, B. (2014). Named data networking. *SIGCOMM Comput. Commun. Rev.*, 44(3):66–73.

Zhang, Y., Afanasyev, A., Burke, J., and Zhang, L. (2016). A survey of mobility support in Named Data Networking. In *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 83–88. IEEE.

Prevendo Número de Requisições a Vídeos Visando Caching Adaptativo: Um Estudo de Caso com Vídeos Educacionais

Priscila Mello Alves, Fabrício Firmino, Daniel Sadoc Menasché

[1]Universidade Federal do Rio de Janeiro (UFRJ)

Resumo. *Mecanismos dinâmicos de alocação de* cache *vêm sendo amplamente utilizados visando melhorar o desempenho de sistemas de distribuição de conteúdo. Tais mecanismos requerem a determinação da quantidade de recursos que devem ser alocados para o atendimento ótimo de requisições considerando restrições de custo. No presente trabalho é proposto um método para previsão do número de requisições a uma aplicação de vídeo educacional. As previsões obtidas com o método proposto podem ser usadas para refinar políticas de alocação de recursos de* cache *em rede. Os resultados encontrados nos experimentos mostram que é possível prever o número de acessos futuros dentro do cenário analisado, e que a suavização exponencial dupla apresenta as melhores predições.*

1. Introdução

Atualmente, a transmissão de vídeo corresponde a mais de 70% do tráfego da Internet em horários de pico [Sandvine 2015]. Uma das formas mais simples de se aumentar o desempenho da distribuição de vídeos online consiste no uso de *caches* distribuídos ao longo da rede. Ao se equipar roteadores com *caches*, quando uma requisição chega ao roteador esta pode ser imediatamente servida, diminuindo o tráfego na rede e o tempo de resposta aos clientes.

A principal motivação deste trabalho advém de infraestruturas de *cache* compartilhado, que permitem o dimensionamento dinâmico da quantidade de *cache* disponibilizada aos diferentes usuários. Em tais infraestruturas, cada usuário pode, dinamicamente, requisitar e alocar espaço dos diferentes *caches*, incorrendo custos proporcionais ao tempo e espaço utilizados. As plataformas *Amazon ElastiCache* [Amazon 2015] e *Memcached Cloud* [Labs 2017] já permitem que seus usuários dimensionem, de forma dinâmica, a quantidade de *cache* utilizada.

Duas etapas compõem o processo para dimensionamento ótimo de *caches*: a previsão do número de requisições e a definição de uma política para alocação de recursos. O objetivo do presente trabalho é criar um método de predição do número de requisições que devem ser atendidas. Para isso, utiliza-se um *dataset* composto por vídeos educacionais produzidos por alunos do curso de Avaliação de Desempenho da UFRJ e disponibilizados no *Youtube* [UFRJ]. Este canal de vídeos conta com mais de 200 mil visualizações e possui características muito peculiares, como periodicidade em diferentes níveis de granularidade (vide Figura 1).

A principal contribuição do presente trabalho consiste na análise de séries temporais e previsão do número de visualizações para cada vídeo no canal educacional considerado. As séries temporais analisadas possuem componentes cíclicas explícitas. A confirmação da presença dessas componentes foi obtida através da aplicação de testes

estatísticos de estacionariedade e tendência às séries. A partir de tais análises, obteve-se um direcionamento dos melhores métodos de regressão a serem utilizados. A Regressão Lasso [Hans 2009], a Suavização Exponencial Simples e a Suavização Exponencial Dupla [Hyndman et al. 2008] foram pré selecionadas, para fins de regressão, tendo a última gerado o menor erro médio quadrático na previsão.[1]

O presente trabalho está organizado da seguinte forma: na Seção 2 são apresentados os trabalhos relacionados da área; na Seção 3 é descrito o método proposto para previsão de séries temporais e apresentam-se os resultados obtidos; na Seção 4 apresentamos as conclusões e possíveis direções de trabalhos futuros.

2. Trabalhos Relacionados

A literatura sobre sistemas de *cache* é vasta [Zhang et al. 2013]. Recentemente, o interesse em redes de *cache* tem aumentado em função das arquiteturas de Internet do futuro baseadas em redes orientadas a conteúdo. A literatura sobre dimensionamento de *caches* (*cache dimensioning*) também é ampla [Carofiglio et al. 2011, Bilchev et al. 1999, Ciccarella et al. 2014, Kalla and Sharma 2016, Carofiglio et al. 2011, Zhang et al. 2013, Bilchev et al. 1999, Ciccarella et al. 2014, Kalla and Sharma 2016], incluindo trabalhos sobre dimensionamento estratégico usando *leases* [Ma and Towsley 2015] e trabalhos relacionando previsão de popularidade de conteúdo e mecanismos de *caching* [Li et al. 2016]. Entretanto, não é de conhecimento dos autores do presente trabalho referências anteriores que abordem o dimensionamento dinâmico de *caches* em função dos padrões (possivelmente cíclicos) encontrados nas séries temporais de requisições. Tomou-se então proveito dos padrões periódicos das séries de requisições a vídeos educacionais no *Youtube* para predizer o número de requisições, e vislumbra-se trabalho futuro que faça uso de tais predições com objetivo de sugerir novas formas de alocação de recursos de *cache* em rede.

3. Experimentos e Resultados

A seguir, são apresentadas a base de dados utilizada e algumas de suas propriedades. Em seguida, os resultados dos testes estatísticos aplicados bem como o desempenho de diferentes modelos de previsão considerados são descritos.

3.1. Base de Dados

A base de dados utilizada foi obtida no canal do *YouTube* Avaliação de Desempenho (UFRJ). Os dados são obtidos através da ferramenta *YouTube Recommender* e a coleta efetuada em 13/03/2017. O canal possui um total de 35 vídeos e 287.039 visualizações. A Tabela 1 apresenta um sumário de informações sobre os vídeos do canal, incluindo duração do vídeo e número de visualizações para os cinco vídeos com mais acessos acumulados. Para a realização dos experimentos utilizou-se os cinco vídeos com o maior número de visualizações.[2]

Por tratarem de conteúdo educacional, os cinco vídeos considerados têm o número de *views* com características cíclicas bem marcantes tanto ao longo dos meses como

[1]Uma versão estendida deste trabalho encontra-se em `https://tinyurl.com/cachealvespriscila`.

[2]Os dados utilizados neste trabalho estão disponíveis em `https://tinyurl.com/dadosyoutube`.

Nome do Vídeo	Duração do Vídeo	Número de Views
Probabilidade Condicional	15:54	80.038
Distribuições Discretas	18:34	59.313
Teorema de Bayes	12:56	43.592
Teorema Central do Limite	10:26	17.197
Distribuição Exponencial	11:35	10.723
Demais vídeos	10:01 (média)	77.953 (total)

Table 1. Sumário do Canal Avaliação de Desempenho

ao longo dos dias de cada semana. A Figura 1 apresenta o número de *views* ao longo do tempo, correspondentes a dois dos vídeos utilizados, Probabilidade Condicional e Distribuições Discretas.

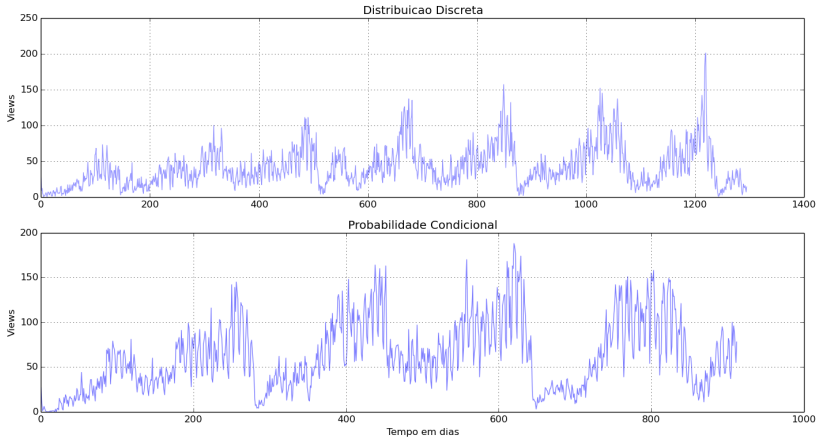


Figure 1. Número de Visualizações ao longo do tempo

3.2. As Séries Temporais São Estacionárias e Com Tendência (*Drift*)

Para as análises estatísticas foram utilizados os testes Dickey-Fuller Aumentado [Cheung and Lai 1995] para o estudo da estacionariedade e o teste de Cox-Stuart [Chang 1991] para a análise de tendência. Os objetivos são determinar (1) se as séries são ou não estacionárias, e (2) se possuem ou não tendência. Como critério de decisão utilizou-se o *p-valor* que pode ser interpretado como o menor nível de significância no qual se rejeitaria a hipótese nula. Os resultados obtidos encontram-se na Tabela 2.

O teste de Dickey-Fuller Aumentado foi aplicado às cinco séries de estudo. Para todos os casos, o *p-valor* encontrado foi muito pequeno e a hipótese nula de não estacionariedade, é rejeitada para qualquer nível de significância. Portanto todas as séries de estudo são estacionárias, ou seja, se desenvolvem aleatoriamente ao redor de uma média (não necessariamente fixa) e com variância constante.[3]

No teste de Cox-Stuart, para testar a presença da componente tendência, os p-*valores* obtidos foram muito pequenos. Portanto, a hipótese nula, que considera ausência de tendência, é rejeitada para qualquer nível de significância em todos as séries, ou seja, todas as séries apresentam tendência. Tal tendência pode ser facilmente observada na Figura 1, onde nota-se que, uma vez fixado o dia do ano, em geral cada vídeo recebe

[3]Na literatura, geralmente estacionariedade significa estacionariedade fraca, onde há apenas restrições com relação aos segundos momentos serem finitos. Assim, uma série temporal é considerada estacionária se flutua aleatoriamente em torno de uma média, refletindo alguma forma de equilíbrio estatístico estável.

um número crescente de visualizações por dia ao longo dos aproximadamente três anos considerados.

Série Temporal	Teste ADF	Teste Cox Stuart
Probabilidade Condicional	*1,84e-16*	*2,411e-07*
Distribuições Discretas	*1,27e-17*	*4,783e-09*
Teorema de Bayes	*9,19e-14*	*6,383e-05*
Teorema Central do Limite	*6,63e-25*	*3,313e-05*
Distribuição Exponencial	*1,12e-19*	*2,731e-04*

Table 2. p-valor dos Testes Estatísticos

3.3. A Suavização Exponencial Dupla Gera Melhores Predições

A escolha do modelo foi realizada em duas etapas. A primeira etapa consistiu em otimizar os parâmetros de cada modelo individualmente, para todas as séries de estudo, usando como referência o erro quadrático médio (*MSE*). Para cada série, os dados foram separados em três grupos: treino, validação e teste, contendo as primeiras 50% observações, e as subsequentes 30% e 20% observações associadas a cada série, respectivamente.

Para cada uma das séries, a etapa de otimização dos parâmetros foi realizada primeiro com os dados de treino. Em seguida, os dados de teste alimentaram o processo de otimização para verificar a concordância dos parâmetros com os encontrados nos dados de treino, o que ocorreu para todas as séries. Posteriormente, já com os parâmetros escolhidos, verificou-se qual dos modelos está associado aos menores valores de *MSE* para os dados de validação.

Na Regressão Lasso foram testadas diferentes hipóteses, tanto lineares quanto não lineares. O melhor ajuste foi obtido com o uso conjunto de 3 hipóteses: uma média móvel curta, que usa 2 dias anteriores à observação que se deseja prever; uma média móvel longa, que utiliza 5 dias anteriores e a média simples de todas as observações anteriores.

Na Suavização Exponencial Simples define-se Y_i como a observação i original e $\widehat{Y}_i$ como a observação i estimada. Assume-se que $\widehat{Y}_t = \alpha Y_{t-1} + (1-\alpha)\widehat{Y}_{t-1}$. O parâmetro que gerou melhor ajuste, para todas as séries, foi α = 0,5, que sugere uma velocidade de amortecimento moderada.

A Suavização Exponencial Dupla (Modelo de *Holt*) considera e suaviza a componente de tendência da série e possibilita a previsão de m passos a frente do ponto de regressão. Para tal, define-se γ como sendo o fator de suavização para a tendência, l_t como o nível no tempo t e b_t como a tendência no tempo t. As equações de nível, tendência e estimação são então definidas por

$$l_t = \alpha\, Y_t + (1-\alpha)\,(l_{t-1} + b_{t-1}) \tag{1}$$

$$b_t = \gamma\,(l_t - l_{t-1}) + (1-\gamma)\, b_{t-1} \tag{2}$$

$$\widehat{Y}_{t+m|t} = l_t + m b_t \tag{3}$$

Foram otimizados os parâmetros de suavização da observação e de suavização da tendência considerando a previsão de 1 passo à frente, ou seja, no momento t estima-se a observação do tempo $t+1$. O melhor ajuste encontrado para as séries Probabilidade Condicional, Distribuições Discretas e Teorema Central do Limite consistiu no uso

do parâmetro de suavização da observação α = 0,95 e parâmetro de ajuste de tendência γ = 0,1. Para as séries Teorema de Bayes e Distribuição exponencial o parâmetro de suavização da observação que melhor se ajustou foi α = 0,96 e o parâmetro de ajuste de tendência γ = 0,1.

Os *MSE* encontrados para cada modelo testado em cada série encontram-se expostos na Tabela 3. O modelo de Suavização Exponencial Dupla foi o que melhor se ajustou a todas as séries, retornando *MSE* significativamente menor do que os outros modelos testados. Isto ocorre porque o modelo de Suavização Exponencial Dupla contempla a presença de tendência nas séries.

Série Temporal	Regressão Lasso	Suavização Simple	Suavização Dupla
Probabilidade Condicional	644,75	439,19	*5,64*
Distribuições Discretas	357,15	225,20	*3,38*
Teorema de Bayes	456,28	296,47	*3,28*
Teorema Central do Limite	61,67	36,15	*0,24*
Distribuição Exponencial	39,27	26,01	*0,22*

Table 3. Comparação do *MSE* dos Modelos

A fim de exemplificar graficamente a diferença no ajuste de cada modelo, a Figura 2 apresenta a curva original, bem como as previsões e os erros quadráticos ponto a ponto de cada um dos modelos testados para a série Probabilidade Condicional. Vale ressaltar que as escalas usadas no eixo vertical, que representa o número de *views*, são diferentes nos três gráficos apresentados na Figura 2. No gráfico, a linha azul representa os dados originais, a verde o ajuste e a vermelha o erro. Note que as curvas verde e azul quase coincidem no gráfico referente à Suavização Exponencial Dupla. O modelo de Suavização Exponencial Dupla apresenta erros quadráticos médios menores e mais estáveis, com alta concentração entre 0 e 50 – correspondendo a um erro ponto a ponto próximo a 7.

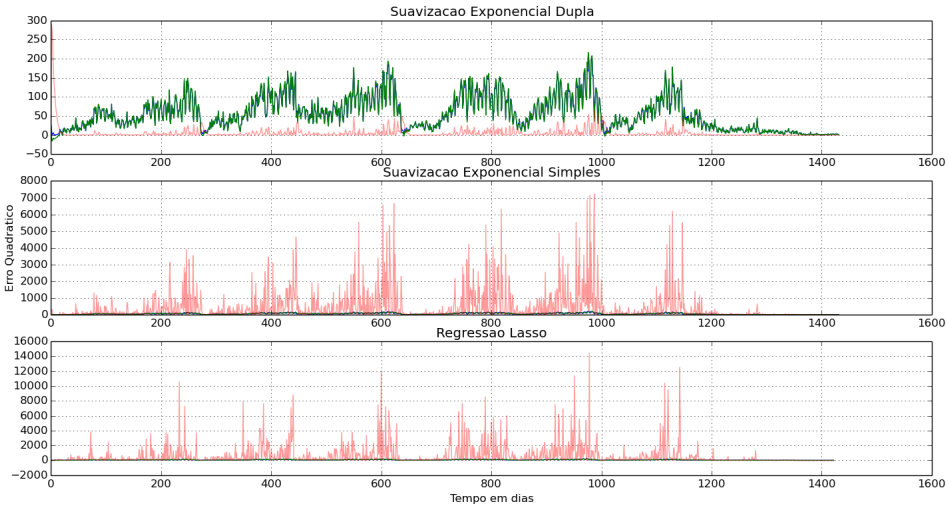


Figure 2. Erro Quadrático dos Modelos de Previsão Analisados para o Vídeo Probabilidade Condicional

4. Conclusão

Os testes estatísticos empregados mostraram que as séries utilizadas de número de visualizações a vídeos educativos são estacionárias e consequentemente convergentes, o que garante bons resultados da previsão a longo prazo. A presença da componente de tendência em todas as séries foi comprovada através também de testes estatísticos e indicou que o uso de um modelo de regressão que contemplasse a mesma é mais adequado. A Suavização Exponencial Dupla, modelo que utiliza a tendência, mostrou-se o melhor método de previsão das séries. Como trabalho futuro, pretende-se definir uma política de alocação de recursos de *caching* para vídeos educativos que faça uso dos modelos preditivos estudados neste trabalho.

References

Amazon, E. (2015). Amazon web services. *Available in: `http://aws.amazon.com/es/ec2/` (Maio 2017)*.

Bilchev, G., Marshall, I., Roadknight, C., and Olafsson, S. (1999). Modelling and performance analysis of cache networks. *Proc UKPW*.

Carofiglio, G., Gehlen, V., and Perino, D. (2011). Experimental evaluation of memory management in content-centric networking. In *ICC*, pages 1–6. IEEE.

Chang, H.-C. (1991). *Trend test: comparison of the Wilcoxon Rank Sum Test and the Cox-Stuart Test*.

Cheung, Y.-W. and Lai, K. S. (1995). Lag order and critical values of the augmented Dickey–Fuller test. *Journal of Business & Economic Statistics*, 13(3):277–280.

Ciccarella, G., Roffinella, D., Vari, M., and Vatalaro, F. (2014). Performance improvement and network TCO reduction by optimal deployment of caching. In *Euro Med Telco Conference (EMTC), 2014*, pages 1–6. IEEE.

Hans, C. (2009). Bayesian lasso regression. *Biometrika*, pages 835–845.

Hyndman, R., Koehler, A. B., Ord, J. K., and Snyder, R. D. (2008). *Forecasting with exponential smoothing: the state space approach*. Springer Science & Business Media.

Kalla, A. and Sharma, S. K. (2016). A constructive review of in-network caching: A core functionality of ICN. In *ICCCA*, pages 567–574. IEEE.

Labs, R. (2017). Memcached cloud — Redis Labs.

Li, S., Xu, J., van der Schaar, M., and Li, W. (2016). Popularity-driven content caching. In *INFOCOM*, pages 1–9. IEEE.

Ma, R. T. and Towsley, D. (2015). Cashing in on caching: On-demand contract design with linear pricing. In *CONEXT*, page 8. ACM.

Sandvine (2015). More than 70% of internet traffic during peak hours now comes from video and music streaming. `http://www.businessinsider.com/`.

UFRJ. Avaliação de desempenho UFRJ, year = 2017, note = `https://www.youtube.com/user/adufrj20121` accessed: 2016-09.

Zhang, G., Li, Y., and Lin, T. (2013). Caching in information centric networking: A survey. *Computer Networks*, 57(16):3128–3141.

XIII Workshop de Redes P2P, Dinâmicas, Sociais e orientadas a Conteúdo (WP2P+)

SBRC 2017

Sessão Técnica 2 – Redes Sociais

Explorando a teoria de grafos e redes complexas na análise de estruturas de redes sociais: Um estudo de caso com a comunidade online Reddit

Felipe Taliar Giuntini e Jó Ueyama

[1]Instituo de Ciências Matemáticas e de Computação - ICMC/USP
Universidade de São Paulo
São Carlos – SP – Brazil

felipegiuntini@usp.br, joeyama@icmc.usp.br

Abstract. *Social networks have become a commonly used environment for sharing personal information. Through them, many feel more willing to share their ideas, thoughts and opinions. In this context, the large volume of data disseminated in the network allow to conduct social studies in order to understand behavioral aspects of community life. This study explores a set of techniques and algorithms in the area of complex and statistical networks with the purpose of analyzing the structure of the Reditt virtual social network. Through this analysis it was possible to demonstrate that the network is stable in relation to time and that it possesses a great diversity of subcommunities, but many isolated and that do not interrelate. This may indicate a lack of influencers and a tendency for network segregation.*

Resumo. *Redes Sociais se tornaram um ambiente comumente utilizado para compartilhamento de informações pessoais. Por meio delas, muitos se sentem mais a vontade para compartilhar suas ideias, pensamentos e opiniões. Neste contexto, o grande volume de dados divulgados na rede permitem realizar estudos sociais em busca de entender aspectos comportamentais da vida em comunidade. Este estudo explora um conjunto de técnicas e algoritmos da área de redes complexas e estatística com o objetivo de analisar a estrutura da rede social virtual Reddit. Por meio desta análise foi possível demonstrar que a rede é estável em relação ao tempo e que há uma grande diversidade de subcomunidades, porém isoladas. Isso pode indicar a falta de influenciadores e uma tendência a segregação na rede.*

1. Introdução

As relações sociais e o trabalho em rede são componentes fundamentais da vida humana e têm sido historicamente ligados de acordo com as limitações de tempo e espaço, embora essas restrições tem sido parcialmente removidas devido à evolução tecnológica, principalmente da Internet e sua difusão de uso.

O surgimento de tecnologias Web e sua evolução permitiram o oferecimento de serviços em redes sociais virtuais do mesmo modo que organizam de forma não virtual. Essa noção de rede social e seus métodos de análise atraíram grande interesse e curiosidade da comunidade em geral, principalmente de estudiosos das áreas de ciência social

e comportamental nas últimas décadas. Isso se deve ao fato das redes sociais fornecerem uma poderosa abstração da estrutura e da dinâmica de diversos tipos de pessoas ou interação pessoa-tecnologia. Desse modo, a análise da rede social pode indicar o estudo da estrutura social virtual e seus efeitos para analisar aspectos sociais e culturais.

Neste contexto, entende-se a Rede Social Virtual como um conjunto de atores (nós) e um conjunto de relacionamentos conectando esses atores, ou seja, arestas [Tindall and Wellman 2001]. Pode-se compreender um nó como diversos componentes de uma rede, como por exemplo, os usuários e as postagens. Enquanto isso, são exemplos de arestas, as amizades,*likes*, compartilhamentos, dentre outros. Como na vida real, é dessa forma que são construídas as comunidades nas redes sociais, por meio de relacionamentos.

Inúmeras abordagens de diversas áreas do conhecimento tem sido desenvolvidas com o objetivo de compreender melhor os padrões de comportamento e a estruturas presentes nas redes sociais virtuais. Com isso, este trabalho explora o uso de conjunto de métricas e abordagens das áreas da teoria de grafos, redes complexas e estatística com o objetivo de compreender a estrutura da comunidade virtual Reddit.

Para atingir o objetivo proposto é apresentado na seção 2 um plano de fundo sobre a teoria de grafos e redes complexas e posteriormente na seção 3 é discutido o estudo de caso, com a base de dados utilizada e os resultados da aplicação de diferentes métricas de análise da área.

2. Teoria de Grafos e Redes Complexas

Aproveitando-se dos principais conceitos da estatística, sistemas dinâmicos e teoria dos grafos, as Redes Complexas despertam interesse de diversas áreas do conhecimento tais como física, matemática, biologia, medicina e sociologia. Isso deve-se a diversidade de aplicações sobre uma grande variedade de problemas, os quais incluem redes socias, redes biológicas, internet, dentre outros [STROGATZ 2001]; [Albert and Barabási 2002]; [Newman 2003]; [Boccaletti et al. 2006]; [Fortunato 2010]; [Newman 2010].

Como a topologia dessas redes não são intuitivas, não regulares e nem completamente aleatórias, elas são denominadas redes complexas. A literatura possui muitas medidas e modelos para caracterizar a estrutura dessas redes. Essas medidas podem ser usadas para analisar as propriedades estatísticas que descrevem a estrutura e o comportamento de sistemas em rede, enquanto a criação de modelos de rede está normalmente relacionada ao entendimento do significado dessas propriedades.

Exemplos de medidas de rede bastante conhecidas incluem a modularidade e o PageRank ([Newman and Girvan 2004]; [Page et al. 1999]). A primeira é muito explorada para a tarefa de detecção de comunidades, uma vez que ela mede a divisão de uma rede em grupos, e a segunda é a medida ranqueamento da ferramenta de busca do Google, com o objetivo caracterizar a importância de páginas Web.

Em relação aos modelos de redes complexas, dentre os mais conhecidos estão as Redes Pequeno Mundo e as Redes Livres de Escalas, dentre os quais possuem características estruturais peculiares [Watts and Strogatz 1998]; [Barabási et al. 2000]; [Pastor-Satorras and Vespignani 2001]. Enquanto o primeiro possui elevado agrupamento e proximidade entre os nós, o segundo é caracterizado por uma lei de potência.

Ao contrário de boa parte dos modelos de redes, em que são descritos em função de mecanismos de crescimento, outro tópico relevante em redes complexas considera que alguns problemas reais podem ser mais bem explicados pela otimização estrutural de redes [Newman 2010]

Em redes complexas, o termo rede denota o conceito informal que descreve um objeto composto de elementos e as conexões entre estes elementos. Tomando como exemplo uma rede social, os elementos estão, normalmente, associados às pessoas, enquanto as conexões podem estar associadas às relações de amizade entre elas. Matematicamente, a forma natural de modelar estas redes é a partir dos conceitos de grafos [Bollobás 1998].

Um grafo ou rede $G = (V; E)$ é uma estrutura matemática composta por dois conjuntos finitos V e E, onde V é o conjunto de n vértices (ou nós) e E o conjunto de m arestas (ou conexões) do grafo. Cada vértice do grafo é normalmente identificado por um valor inteiro ordenado $i = 1; 2; :::; n$, enquanto a conexão entre dois nós i e j é representada por $(i; j)$, ou seja $E \subseteq (i; j) \mid i, j \in V$. De acordo com o tipo de aresta admitido, os grafos podem ser classificados em direcionados, não direcionados ou mistos [STROGATZ 2001].

Pelo que é conhecido na literatura, redes complexas engloba um grande conjunto de medidas de rede, que possuem diversas aplicações em sistemas reais e são oriundas de estudos do campo da estatística, sistemas complexos, matemática, sistemas não lineares, entre outros . Dentre as medidas tem-se Grau, Assortividade, Coeficiente de Agrupamento, Proximidade, Intermedialidade, Modularidade, *PageRank* [Newman 2003]; [Costa et al. 2007].

O desejo de modelar propriedades e dinâmicas de rede, com o objetivo de entender e reproduzir o comportamento de vários sistemas reais motiva diretamente o estudo de redes complexas. Muitas investigações teóricas e empíricas sobre redes reais, tais como [Barabási and Albert 1999], [Watts and Strogatz 1998], [Newman 2010] culminaram no desenvolvimento de modelos de rede que refletem de forma comportada características próprias desses sistemas e que se constituem em uma "caixa de ferramentas" para a análise de vários outros sistemas complexos relacionados. As principais classes de modelagem são: Redes Aleatórias, Redes Pequeno Mundo, Redes Livres de Escala, Redes Modulares e Otimização Estrutural de Redes.

3. Estudo de Caso com a comunidade online Reddit

A Reddit é uma plataforma de rede social em que os membros registrados podem enviar conteúdo, como mensagens ou mesmo submeter links diretamente. Essas submissões são votadas positivamente ou negativamente pelos usuários da rede, de modo que as postagens podem subir ou descer em um ranking, ou seja, as postagens com melhor score permanecem na primeira página ou no topo de uma categoria, denominada *subreddits*, que incluem notícias, ciência, jogos, filmes, músicas, livros, fitness, comida, compartilhamento de imagens, dentre outros.

Segundo o site *Alexa Traffic Ranks*, a Reddit alcançou em 2017 mais de 234 milhões de usuários cadastrados em sua base e com uma média de 542 milhões de visitantes mensais únicos, ocupando a 4ª posição em número de acessos nos Estados Unidos da América e a 17ª em nível global [Alexa Internet 2017].

3.1. Base de dados

Este conjunto de dados é uma coleção de 132.308 submisssões na plataforma *reddit.com* [Lakkaraju et al. 2013]. Cada postagem é caracterizada por uma série de atributos que podem ser conferidos a seguir:

- **image_id:** refere-se ao número de identificação da imagem, ou seja, submissões com mesmo id, são a mesma imagem.
- **unixtime:** horário da submissão
- **rawtime:** horário em formato texto bruto
- **title:** título da submissão
- **total_votes:** (number_of_upvotes:) + (number_of_downvotes)
- **reddit_id:** número de identificação da submissão na reddit, por exemplo: reddit.com14c3ls
- **number_of_upvotes:** número de votos positivos
- **subreddit:** sub-tópico do reddit, por exemplo,`reddit.com/r/pics/`
- **number_of_downvotes:** número de votos negativos
- **localtime:** horário local da submissão (unix time)
- **score:** n(number_of_upvotes:) - (number_of_downvotes)
- **number_of_comments:** número de comentários que a submissão recebeu
- **username:** nome do usuário que submeteu a imagem, por exemplo: www.reddit.com/user/thatseffedup

Para [Lakkaraju et al. 2013] essa base de dados representa uma experiência natural de grande escala, permitindo desvendar a qualidade inerente ao conteúdo e realizar análises mais complexas da rede. Isso se deve ao fato de que a base considera que uma mesma imagem pode ser submetida com títulos e em categorias diferentes.

3.2. Métricas e Avaliação

Considerando o grande conjunto de dados e um grande número de submissões referente uma mesma imagem, realizou-se uma operação de redução do conjunto de dados, com o objetivo auxiliar no processamento e tornar análise da rede viável. Desde modo, postagens com mesmo *image_id* foram agrupadas como uma única submissão. Contudo, para manter a qualidade da análise foi mantido o título da postagem com maior *score* e realizada a média dos outros atributos, como *upvotes*, *downvotes* e *score*.

Com o objetivo de estabelecer o grafo da rede, as postagens (nós) de um mesmo período foram conectadas formando um grafo direcionado. Sendo que, dado que uma postagem $P(n)$ possuí um score maior que a postagem $P(m)$ no mesmo intervalo de tempo t, então $P(n)$ possuí uma aresta direcionada no sentido $P(n) \rightarrow P(m)$. Neste caso, considerou-se como período de tempo, o período de um mês, sendo que cada mês recebeu uma cor diferente.

O contexto formado para essa análise é um grafo misto, composto por 16.734 nós e 14.607 arestas direcionadas. Inicialmente, por meio da Figura 1 que apresenta uma visão externa da estrutura geral da rede, é possível perceber que não há um intervalo de tempo mais expressivo do que outro no que tange o número de submissões, tendo em vista que a rede é praticamente uniforme nesse sentido. Contudo, não é possível obter outras informações revelantes da sua estrutura com essa representação geral, devido a complexidade e densidade do grafo.

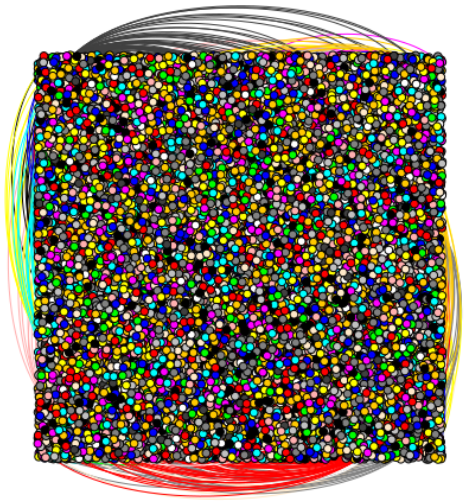


Figura 1. Visão Geral da Rede

Com isso, explora-se um conjunto de medidas e algoritmos de teoria de grafos, estatística e redes complexas com o objetivo de compreender melhor os comportamentos sociais que constituem essa estrutura.

3.2.1. Distância do Grafo: Distribuição da excentricidade e centralidade da proximidade

Estimar o índice de centralidade é parte essencial do processo de análise de rede sociais. Com isso, motivados pelo crescente interesse em calcular índices de centralidade em redes de grande escala e resolver o problema de custo computacional existente na época, Ulrik Brandes propôs em [Brandes 2001] novos algoritmos de centralidade, que requerem espaço de $O(n+m)$ e executam em $0(nm)$ e $0(nm+n2logn)$ em medidas de tempo em redes não ponderadas e ponderadas, respectivamente, onde m é o número de conexões, ou seja, arestas.

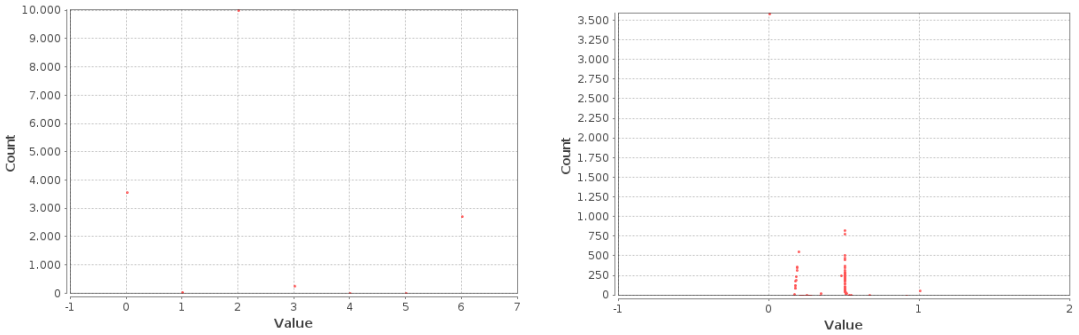
Neste estudo de caso calculou-se a distribuição da excentricidade e a centralidade de proximidade [1]. A excentricidade $\epsilon(v)$ de um vértice v em um grafo conectado G é a distância de gráfico máxima entre v e qualquer outro vértice u de G. Para um gráfico desconectado, todos os vértices são definidos como tendo excentricidade infinita [West 2000]. Ou seja, a excentricidade máxima é o diâmetro do gráfico e a excentricidade mínima do grafo pode ser entendido como o raio do grafo. Já a centralidade de proximidade foi inicialmente definida por [Sabidussi 1966] da seguinte forma:

$$ClosenessCentrality(V) = \frac{1}{\sum_{t \in V} dG(v,t)}$$

Os resultados da execução dos algoritmos proposto por [Brandes 2001] acima demonstram que a rede analisada possuí diâmetro 6, ou seja, dado um nó inicial na rede

[1] respectivamente em inglês: *Closeness Centrality Distribution* e *Exccentricity Distribution*

são necessários até 6 passos para alcançar o nó mais distante na rede, comprovando a conhecida teoria de Pequeno Mundo[Watts and Strogatz 1998]. Já o tamanho médio do caminho, isto é, a a frequência que um determinado nó aparece nos caminhos mais curtos entre nós da rede é de 4,47. Ambas informações estão disponíveis na Figura 2.



(a) Excentricidade (b) Centralidade da proximidade

Figura 2. Distribuição da rede (a) e (b)

3.2.2. Distribuição *Hub* e *Authority*

A pontuação de *hub* e de autoridade proposta por [Kleinberg 1999] refere-se a importância relativa de um vértice em uma rede. Um vértice possuí maior pontuação *hub* ou autoridade se ele tem um maior *indegree* ou *outdegree* respectivamente. Além de estar conectado a outros vértices com altas pontuações. Nesta análise os nós apresentaram pontuações de *hub* igual a zero e de autoridade 0,042. Ou seja, os nós possuem certa igualdade em relação a importância e uma influência pequena em relação a outros nós na rede, conforme pode-se observar na Figura 3.

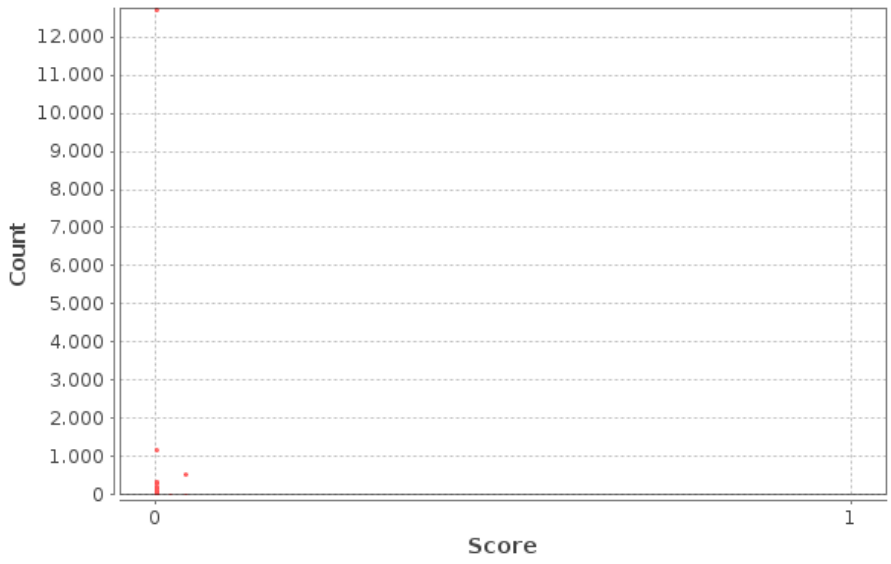


Figura 3. Authority

3.2.3. Identificação e Distribuição de comunidades

Com objetivo de identificar comunidades no grafo explorado, aplicou-se o algoritmo de modularidade proposto por [Blondel et al. 2008], que utiliza a resolução de [Lambiotte et al. 2008]. Assim, ativou-se o modo aleatório, uma vez que produz uma decomposição melhor, embora aumente o tempo de processamento. Além disso, considerou-se o peso das arestas e uma resolução de 1.0 como parâmetro. Neste caso, encontrou-se um índice de modularidade de 0,971, mostrando que o grafo está bem completo, já que está bem próximo de 1, que significa a totalidade ou completude de um grafo. Além disso, foram identificadas 3.658 comunidades, cuja distribuição pode ser observada pela Figura 4.

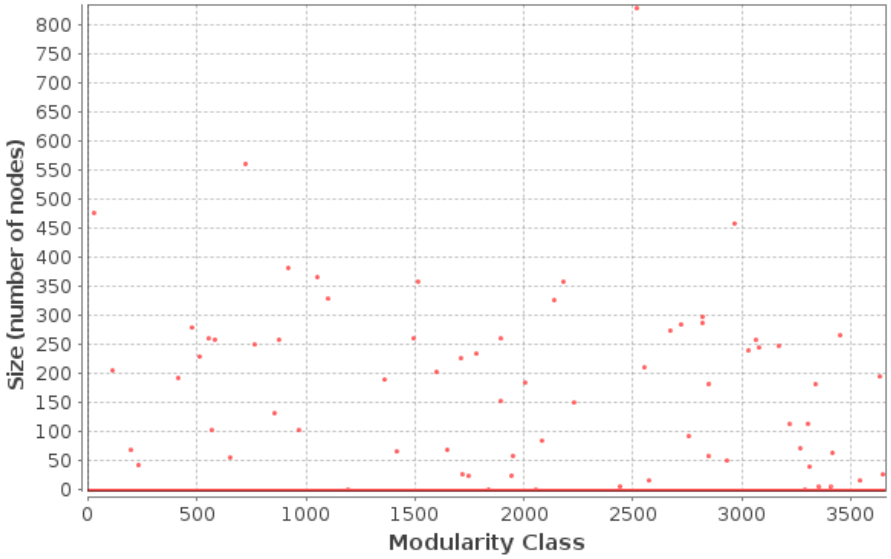


Figura 4. Distribuição de tamanho

Considerando que o grafo analisado possuí 16.734 nós e que foram identificadas 3.658 sub-comunidades obtém-se um índice de 4,57, valor bem próximo ao caminho médio encontrado na seção 3.2.1. Uma rede social com alto número de comunidades pode ser interessante dependendo do ponto de vista. Contudo, o que denota atenção é que este alto número de sub-grupos pode indicar um alto nível de segregação na rede.

No que tange a Reddit, essa segregação se deve ao fato da rede social possuir *sub-reddits*, que são grupos destinados a um determinado assunto, como, por exemplo, jogos, música, eventos, dentre outros. Ou seja, percebe-se que os as postagens estão mais direcionadas a um público específico interessado, do que na linha de propósito geral. Isso se deve ao fato de que em grupo específico, a postagem tem maiores chances de ter maior visibilidade, uma vez que é possível conseguir um número maior de *up_votes*, já que o assunto é mais restrito.

3.2.4. PageRank

Para a caracterização de importância do nó na rede utilizou-se o PageRank, algoritmo proposto por [Brin and Page 1998] e utilizado na máquina de busca do Google para definir

o grau de importância das páginas Web. Basicamente, é uma medida de centralidade baseada em caminhos aleatórios, onde assume-se que um agente esteja passeando sobre o grafo. Ao visitar determinado nó na rede, o agente pode escolher de modo aleatório alguma das arestas de saída do nó e partir para o nó vizinho. Fazendo o mesmo assim por diante até alcançar todos nós. Além disso, assegurando que o agente não fique preso em um nó sem vértices de saída, o agente pode saltar para qualquer nó do grafo considerando uma probabilidade, e evitando consequentemente problemas de convergência.

O valor de PageRank de determinado nó, pode ser entendido como a probabilidade do agente estar nele, ou seja, quanto maior o número de conexões de entrada de um nó, mais relevante ele é na rede. Além disso, caso os nós que realizam conexões para um outro nó vizinho possuem alto grau de importância, este nó também será altamente relevante.

Nesta análise, para calcular a distribuição do PageRank, utilizou-se como parâmetro uma probabilidade 0.85 para simular a aleatoriedade que um usuário pode acessar determinada postagem na rede social Reddit. Além disso, definiu-se o critério de parada $\epsilon = 0.001$. A distribuição é demonstrada pela Figura 5.

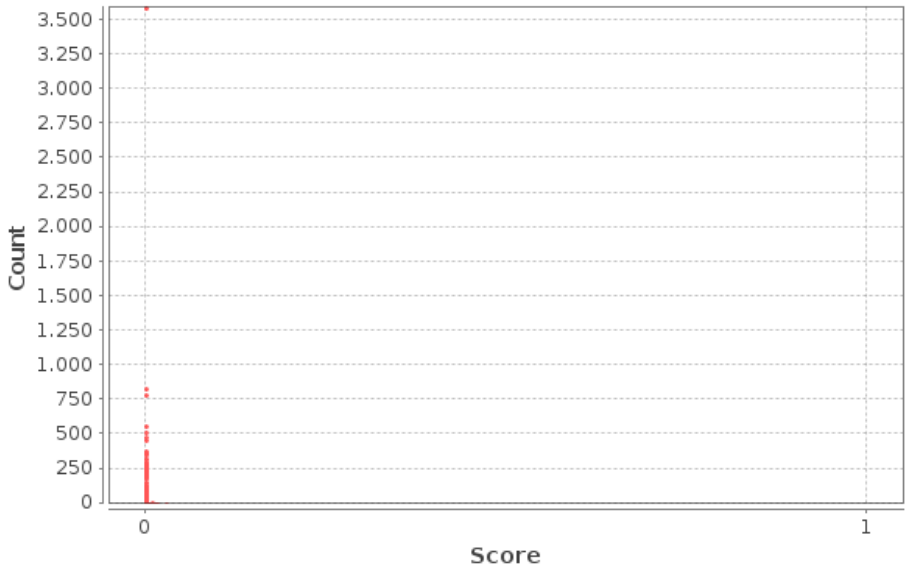


Figura 5. Distribuição do PageRank

3.2.5. Centralidade de autovetor

Proposta por [Bonacich 1987] a centralidade de autovetor é uma medida de centralidade espectral que busca obter propriedades estruturais dos vértices de um grafo a partir das propriedades dos autovalores e autovetores das matrizes associadas a estes grafos. Com base na álgebra linear esta é uma medida de importância do nó baseada em suas conexões, isto é, diferentemente das métricas de centralidade apresentadas na seção 3.2.1, em que é considerado o grau do nó, a centralidade de autovetor pode atribuir alta relevância para um nó com base em sua relação com seus vizinhos, ou seja, mesmo que um determinado nó(u) possuí um baixo grau de centralidade, caso seus vizinhos sejam relevantes, também será atribuída ao nó(u) uma alta centralidade de autovetor.

Os resultados da distribuição da centralidade de autovetor apresentados na Figura 6 levou em consideração como parâmetro uma mudança de soma(*sum change*) aproximada de 0.3424 e 100 interações.

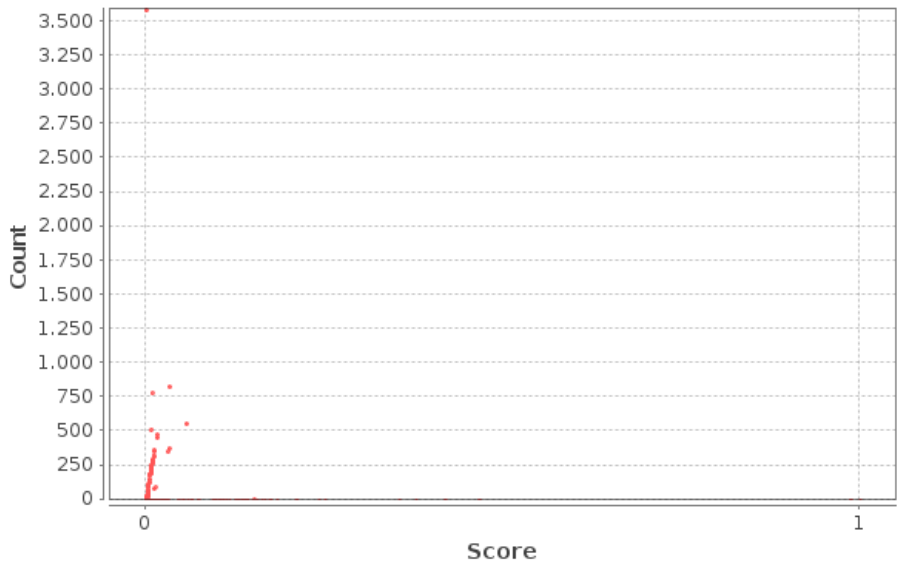


Figura 6. Distribuição da centralidade de autovetor

4. Considerações Finais

Neste trabalho foi explorado o uso de diversas técnicas para análise de estruturas de redes sociais virtuais por meio da aplicação de um estudo de caso com um conjunto de dados de submissões da comunidade online Reddit. Este estudo permitiu compreender melhor estrutura desta rede, como aspectos de centralidade, diâmetro, completude e identificação de comunidades. Neste caso especifico, a divisão da rede em períodos de tempo demonstrou que esta rede social é estável e equilátera, do ponto de vista que as interações foram constantes em todos períodos de tempo.

Outro aspecto importante e curioso que foi demonstrado é que a influência de um nó sobre os outros não tem sido tão significativa. Enquanto isso, notou-se a presença de um vasto número de pequenas sub-comunidades. Isso mostra que as redes estão ficando cada vez mais diversificadas e pequenos nichos tem sido criados. Embora este fator social parece ser positivo, os experimentos demonstraram que o número de influenciadores da rede é pequeno, enquanto a segregação em grupos menores é consideravelmente alta. Isso chama a atenção de cientistas e analistas sociais para refletir os rumos que as redes sociais tem tomado e o quanto isso se reflete na vida em comunidade não virtual.

Contudo, no que tange a experiência deste estudo nota-se que embora haja algoritmos consagrados na literatura, são necessárias novas abordagens que permitem entender e compreender melhor a causa desta enorme diversidade dentro de uma grande rede complexa e o que tem levado este comportamento.

5. Referências

Referências

Albert, R. and Barabási, A.-L. (2002). Statistical mechanics of complex networks. *Reviews of modern physics*, 74(1):47.

Alexa Internet (2017). reddit.com traffic statistics. Disponível em: `http://www.alexa.com/siteinfo/reddit.com`.

Barabási, A.-L. and Albert, R. (1999). Emergence of scaling in random networks. *science*, 286(5439):509–512.

Barabási, A.-L., Albert, R., and Jeong, H. (2000). Scale-free characteristics of random networks: the topology of the world-wide web. *Physica A: Statistical Mechanics and its Applications*, 281(1):69–77.

Blondel, V. D., Guillaume, J.-L., Lambiotte, R., and Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of statistical mechanics: theory and experiment*, 2008(10):P10008.

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., and Hwang, D.-U. (2006). Complex networks: Structure and dynamics. *Physics reports*, 424(4):175–308.

Bollobás, B. (1998). Random graphs. In *Modern Graph Theory*, pages 215–252. Springer.

Bonacich, P. (1987). Power and centrality: A family of measures. *American journal of sociology*, 92(5):1170–1182.

Brandes, U. (2001). A faster algorithm for betweenness centrality. *Journal of Mathematical Sociology*, pages 163–177.

Brin, S. and Page, L. (1998). The anatomy of a large-scale hypertextual web search engine. *Computer networks and ISDN systems*, 30(1):107–117.

Costa, L. d. F., Rodrigues, F. A., Travieso, G., and Villas Boas, P. R. (2007). Characterization of complex networks: A survey of measurements. *Advances in physics*, 56(1):167–242.

Fortunato, S. (2010). Community detection in graphs. *Physics reports*, 486(3):75–174.

Kleinberg, J. M. (1999). Authoritative sources in a hyperlinked environment. *Journal of the ACM (JACM)*, 46(5):604–632.

Lakkaraju, H., McAuley, J. J., and Leskovec, J. (2013). What's in a name? understanding the interplay between titles, content, and communities in social media.

Lambiotte, R., Delvenne, J.-C., and Barahona, M. (2008). Laplacian dynamics and multiscale modular structure in networks. *arXiv preprint arXiv:0812.1770*.

Newman, M. (2010). *Networks: an introduction*. Oxford university press.

Newman, M. E. (2003). The structure and function of complex networks. *SIAM review*, 45(2):167–256.

Newman, M. E. and Girvan, M. (2004). Finding and evaluating community structure in networks. *Physical review E*, 69(2):026113.

Page, L., Brin, S., Motwani, R., and Winograd, T. (1999). The pagerank citation ranking: bringing order to the web.

Pastor-Satorras, R. and Vespignani, A. (2001). Epidemic spreading in scale-free networks. *Physical review letters*, 86(14):3200.

Sabidussi, G. (1966). The centrality index of a graph. 31:581–603.

STROGATZ, S. H. (2001). Exploring complex networks. *Nature, Nature Publishing Group*, 410:268.

Tindall, D. B. and Wellman, B. (2001). Canada as social structure: Social network analysis and canadian sociology. *Canadian Journal of Sociology/Cahiers canadiens de sociologie*, pages 265–308.

Watts, D. J. and Strogatz, S. H. (1998). Collective dynamics of 'small-world'networks. *nature*, 393(6684):440–442.

West, D. B. (2000). *Introduction to Graph Theory*. Prentice-Hall, 2 edition.

XIII Workshop de Redes P2P, Dinâmicas, Sociais e orientadas a Conteúdo (WP2P+)

SBRC 2017

Sessão Técnica 3 – Redes Centradas na Informação e Oportunistas

Distribuindo e Consultando o Estado de Chaves Públicas em Redes Centradas na Informação

Daniel Rezende [1], **Carlos A. Maziero** [1], **Elisa Mannes**[1]

[1]Departamento de Informática – Universidade Federal do Paraná (UFPR)
Caixa Postal 19.081 – 81.531-980 – Curitiba – PR – Brasil

drezende@inf.ufpr.br, maziero@inf.ufpr.br, elisam@inf.ufpr.br

Abstract. *The paradigm of information centric networks (ICN) is an approach to improve the Internet infrastructure and directly support its use, considering named data as a network primitive. In ICN, contents are named by their publishers and should be digitally signed to ensure their integrity and provenance. To sign a content, a publisher should use a public key infrastructure. Once signed, the content is served to customers, which need to retrieve the corresponding public key to validate it. Such keys should be valid in accordance with the rules enforced by the adopted trust model, and should not have been revoked. This paper proposes an architecture to disseminate the current state of the keys used for content validation in ICN. Our approach reduced in up to 41% the average time needed by a client to retrieve the current status of a given key, when compared to a centralized approach.*

Resumo. *O paradigma de redes centradas na informação é uma abordagem para aprimorar a infraestrutura da Internet e apoiar diretamente o seu uso, introduzindo dados nomeados como primitiva de rede. Os conteúdos são nomeados pelos seus publicadores e precisam ser assinados digitalmente para garantir a sua integridade e proveniência. Uma vez assinado, o conteúdo é servido aos clientes que devem obter a chave pública correspondente para validá-lo. Essa chave precisa estar de acordo com as regras impostas pelo modelo de confiança adotado e precisa ser válida, ou seja, não pode ter sido revogada. Este trabalho apresenta uma abordagem para divulgação do estado das chaves utilizadas para validação dos conteúdos. Esta abordagem conseguiu reduzir em até 41% o tempo médio necessário para um cliente consultar a informação do estado de uma chave, em comparação com uma abordagem centralizada.*

1. Introdução

As redes centradas na informação (*Information Centric Networks* - ICN) são caracterizadas por utilizarem conteúdos nomeados, por ter a segurança aplicada diretamente aos conteúdos e por permitir o armazenamento de conteúdos nos elementos do núcleo da rede [Jacobson et al. 2009]. Esse armazenamento permite aos usuários consultar os conteúdos em locais mais próximos à sua localização, reduzindo o tempo de consulta e diminuindo o tráfego da rede.

Nas redes centradas na informação foco principal é o conteúdo, sendo assim, a segurança também é aplicada diretamente aos conteúdos, utilizando assinaturas digitais. A assinatura garante a integridade do conteúdo, ou melhor, garante que o conteúdo não

foi modificado durante o transporte entre a sua origem e destino. Garante também a proveniência, isto é, que o conteúdo realmente foi produzido pelo publicador no qual o usuário confia, independentemente de onde ele foi obtido. Essa relação de confiança pode ser construída através de um modelo de confiança a ser adotado pela aplicação que fará uso da ICN [Jacobson et al. 2009].

Além do modelo de confiança, é necessária uma infraestrutura para gerenciar a criação, distribuição e revogação das chaves criptográficas que serão utilizadas para assinar os conteúdos. Sendo assim, um dos processos fundamentais do gerenciamento de chaves é a revogação e divulgação do estado dessas chaves, tema pouco explorado em ICN. Uma vez que uma chave é revogada, é necessário notificar os seus usuários. Isso pode ser feito de duas formas em um sistema distribuído: enviando essa informação para os usuários ou permitindo que eles a consultem quando necessário.

Considerando esse contexto e o desafio mencionado, este trabalho tem como objetivo analisar uma abordagem de divulgação do estado das chaves criptográficas em ICN. Esta abordagem consiste em utilizar um serviço de consulta de estado de chaves, similar ao que é utilizado hoje na Internet, distribuído e atualizado por replicação. Para avaliar o comportamento do serviço proposto, foram realizados experimentos por meio de simulações utilizando o simulador ndnSim [Mastorakis et al. 2016]. As simulações foram realizadas em um cenário bem próximo da Internet real com o objetivo de medir o tempo de resposta de uma consulta do estado de uma chave. Foram realizados experimentos sem a utilização da abordagem proposta e com a mesma, com um número variável de réplicas do serviço de consulta de estado distribuídas pela rede. Os resultados mostraram uma nítida redução no tempo de resposta para obter o estado de uma chave, que se reduz à medida em que mais réplicas do serviço são adicionadas à rede.

O restante do texto está organizado da seguinte forma. A Seção 2 apresenta uma visão geral das redes centradas na informação e suas características a serem exploradas neste trabalho. A Seção 3 apresenta o processo de revogação de chaves na Internet, como ele é abordado em ICN e os trabalhos relacionados. A Seção 4 traz a descrição detalhada da arquitetura e do funcionamento do serviço de consulta de estados das chaves. A Seção 5 apresenta os experimentos efetuados para avaliar a proposta e analisa os resultados obtidos. Finalmente, a Seção 6 apresenta conclusões e discute possíveis trabalhos futuros.

2. Redes Centradas na Informação

O conceito de Redes Centradas na Informação é uma abordagem comum que designa vários projetos de pesquisa da Internet do Futuro, tendo como base objetos de dados nomeados. O seu objetivo é fornecer um serviço de infraestrutura de rede que seja mais adequado ao uso atual (em particular, distribuição de conteúdo e mobilidade) e mais resiliente a falhas e interrupções [Ahlgren et al. 2012].

No paradigma de ICN, os publicadores da informação podem anunciar a disponibilidade do seu conteúdo, permitindo aos clientes solicitá-lo quando desejarem. Estas primitivas permitem dissociar solicitações e respostas no espaço e no tempo. Em outras palavras, o publicador e o solicitante do conteúdo não precisam saber a localização um do outro, nem precisam estar *online* ao mesmo tempo [Ghodsi et al. 2011].

Das várias arquiteturas de ICN, a NDN (*Named Data Networking*) tem despertado maior interesse dos pesquisadores, por ser uma arquitetura aberta. O projeto NDN foi cri-

ado pela *National Science Foundation* desde 2010, faz parte do Programa de Arquiteturas da Internet do Futuro e tem como objetivo desenvolver uma arquitetura para distribuição de conteúdo.

2.1. Visão geral da NDN

A comunicação em NDN é impulsionada pelos requisitantes de dados, os clientes, através da troca de dois tipos de pacotes: *interesse* e *dados*, cujas estruturas são apresentadas na Figura 1. Quando o cliente deseja obter um determinado conteúdo, ele expressa seu interesse inserindo o nome do conteúdo desejado em um pacote de interesse e o encaminha para a rede. O publicador, ou algum *cache* que possuir este conteúdo, ao receber o interesse encaminhará de volta ao requisitante um pacote de dados em reposta a este pacote de interesse, com o conteúdo solicitado.

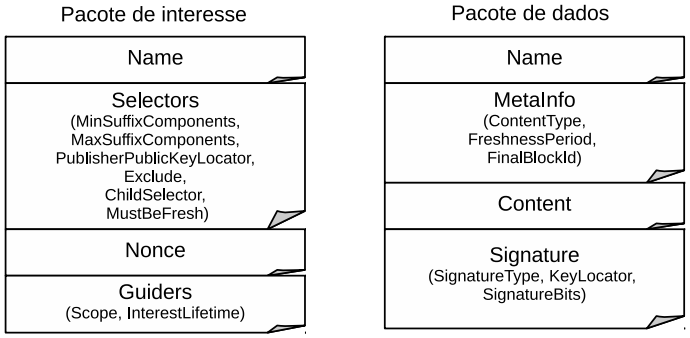


Figura 1. Pacotes na arquitetura NDN (adaptada de [Jacobson et al. 2009], baseada na especificação em [NDN 2014]).

O pacote de interesse possui os seguintes campos:

- *Name*: nome que identifica o conteúdo requisitado;
- *Selectors*: elementos opcionais que qualificam ainda mais dados que podem coincidir com o interesse. Eles são usados para descobrir e selecionar os dados que correspondem melhor ao que a aplicação deseja;
- *Nonce*: carrega uma sequência de caracteres gerados aleatoriamente. A combinação do *Name* e *Nonce* deve identificar exclusivamente um pacote de interesse;
- *Guiders*: especifica opções de comportamento do pacote de interesse, como limites de propagação e tempo de vida.

O pacote de dados possui os seguintes campos:

- *Name*: nome que identifica o conteúdo;
- *MetaInfo*: informações adicionais do pacote de dados, como o tipo de dado que o pacote carrega e o tempo de atualização. Por exemplo, um pacote de dados que carrega informações sobre uma chave possui o valor *KEY* no campo *ContentType*.
- *Content*: conteúdo do pacote, ou seja, os dados propriamente ditos.
- *Signature* : informações sobre a assinatura e localização da chave.

Para encaminhar os pacotes, cada roteador NDN mantém três estruturas: tabela de interesses pendentes (*Pending Interest Table - PIT*), base de informações de encaminhamento (*Forwarding Information Base* - FIB) e um armazenador de conteúdo (*Content*

Store - CS). Essas estruturas são responsáveis pelo recebimento e encaminhamento dos pacotes de interesse e dados. A FIB é uma estrutura semelhante à tabela de roteamento de um roteador IP. Entretanto, ela associa um prefixo de nome a cada interface de saída. Esse prefixo é a identificação do publicador de conteúdo, sendo armazenado na FIB do roteador quando um novo publicador se anuncia para a rede através de um *flooding*. A PIT é uma tabela que armazena os interesses por conteúdos recebidos pelo roteador através de pacotes de interesse. Ela só encaminha para a FIB um único pacote de interesse para o mesmo nome de conteúdo requisitado por um pacote de interesse. O CS tem como função aumentar a eficiência de obtenção dos conteúdos solicitados pelos clientes através do armazenamento dos conteúdos em um *cache* local.

Para requisitar um conteúdo, o cliente deve enviar um pacote de interesse à rede contendo o nome do mesmo juntamente com o prefixo, que é a identificação do publicador. Após receber o interesse, o roteador verifica se esse conteúdo está armazenado no CS. Caso esteja, o roteador gera um pacote de dados para o conteúdo e o envia para a interface de chegada do pacote de interesse. Caso contrário, o roteador verifica se já existe uma entrada em sua PIT para o conteúdo. Se existir, o interesse é agregado, ou seja, sua interface de entrada é armazenada na entrada correspondente na PIT. Caso contrário, ele faz uma busca pelo nome global nas informações de roteamento da FIB. Se uma rota para o interesse for encontrada, uma nova entrada para ele é criada na PIT e o pacote é encaminhado pela interface especificada na FIB. Caso contrário ele descarta o pacote ou envia um NACK[1] para a interface de chegada do pacote de interesse. O processo de tratamento do pacote de interesse é ilustrado na Figura 2.

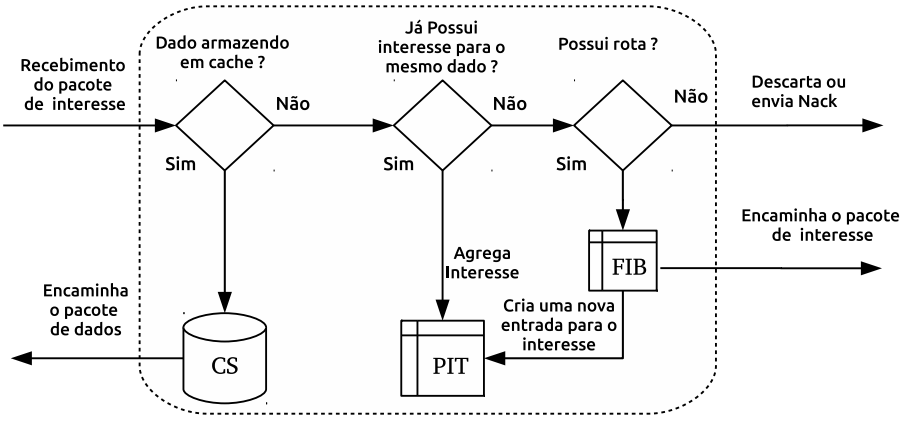


Figura 2. Tratamento de um pacote de interesse em roteador da NDN (adaptada de [Zhang et al. 2014]).

Quando um pacote de dados chega em uma das interfaces de um roteador de conteúdo da NDN, primeiro verifica-se a existência de algum interesse pendente para ele na PIT. Se existir um interesse pendente para esse mesmo conteúdo, de acordo com as políticas de *cache* o seu conteúdo pode ser armazenado no CS, sua entrada correspondente é removida da PIT e o pacote é encaminhado para a interface de destino. Caso não tenha interesse pendente para esse pacote de dados na PIT, o pacote de dados é descartado. Mesmo que não exista interesse pendente para o pacote de dados, e de acordo com as

[1]NACK (*negative-acknowledgement*) é um tipo de mensagem enviada em muitos protocolos de comunicação para reconhecer negativamente ou rejeitar uma mensagem recebida anteriormente.

políticas de *cache*, ele pode ser armazenado no CS. O processo de tratamento do pacote de dados é ilustrado na Figura 3.

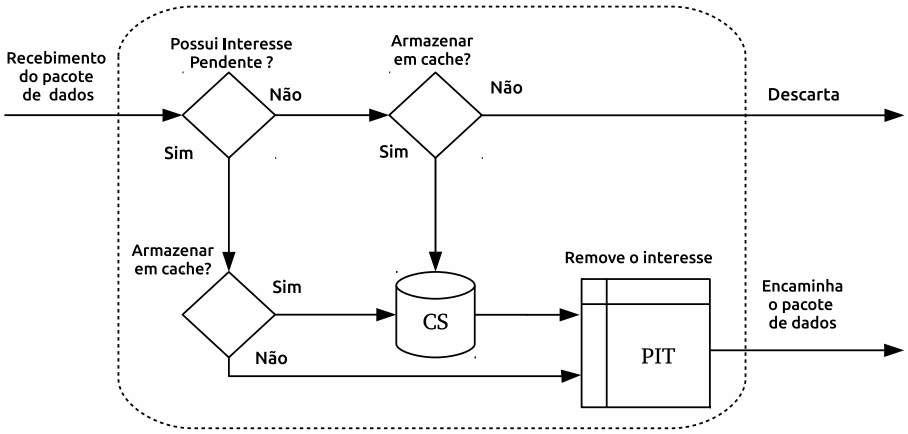


Figura 3. Tratamento de um pacote de dados em roteador da NDN (adaptada de [Zhang et al. 2014]).

2.2. Assinatura dos pacote NDN

Em contraste com as redes TCP/IP, que deixam a responsabilidade pela segurança (ou a falta dela) para os dispositivos, a NDN protege os dados em si, obrigando os publicadores de dados a assinar criptograficamente cada pacote de dados [Jacobson et al. 2009]. Os pacotes de dados são assinados utilizando criptografia de chave pública, também conhecida como criptografia assimétrica. A assinatura é produzida sobre o resultado de uma função de *hash*, que é computado utilizando todos os elementos do pacote de dados, com exceção do campo onde a assinatura é armazenada. Esta assinatura é armazenada no final do pacote, para facilitar sua verificação. Cada pacote de dados assinado contém informações que permitem ao cliente obter a chave pública necessária para verificá-lo. A informação de localização da chave está armazenada no campo *KeyLocator* do pacote de dados.

A assinatura de um pacote tem a função de verificar tanto a integridade do mesmo quanto sua proveniência. Ou seja ela autentica a ligação entre o conteúdo e a chave utilizada pelo produtor para assinar o conteúdo [Jacobson et al. 2009]. O processo de assinatura sozinho não é suficiente para garantir a confidencialidade dos dados. Algum mecanismo externo precisa ser implementado para impedir o acesso indevido às informações que estão sendo carregadas pelo pacote de dados, tendo em vista que esse pacote pode permanecer armazenado em algum *cache* da rede. Para garantir a confidencialidade é necessário utilizar alguma solução que seja capaz de correlacionar um usuário específico com o conteúdo em *cache*. Entre várias soluções propostas podemos mencionar o controle de acesso baseado em reencriptação por *proxy* proposto em [Mannes et al. 2016].

Este trabalho não trata a confidencialidade dos dados, apenas a validação das chaves que serão utilizadas para verificar a integridade e proveniência dos pacotes de dados. Qualquer elemento da rede pode validar um pacote de dados e não apenas os pontos finais da comunicação. Esta verificação mínima é útil para detectar pacotes corrompidos e para a defesa contra ataques na rede. Os roteadores de conteúdo podem optar por verificar todos, alguns ou nenhum dos pacotes de dados. Seus recursos podem permitir que eles se

adaptem dinamicamente, em resposta a um ataque detectado ou a alguma orientação ao cliente [Jacobson et al. 2012].

Para verificar a ligação entre o conteúdo e publicador, a NDN obriga os usuários a adotarem um modelo de confiança específico. A confiança é estabelecida entre publicadores de conteúdo e clientes. O que é apropriado para uma aplicação pode não ser apropriado para outra, sendo assim, os usuários são livres para reutilizar modelos existentes (por exemplo, PKI[2]) para estabelecer a confiança em chaves ou para definir novos modelos mais apropriados para cada tipo de aplicação [Jacobson et al. 2009].

Um modelo de confiança foi proposto para NDN [Yu et al. 2015] composto por regras e esquemas de confiança. Expressões regulares são utilizadas para definir as regras entre os elementos envolvidos. Esse modelo funciona de forma independente de aplicação e vem sendo utilizado para prover o gerenciamento de confiança em diversas aplicação da NDN. O presente trabalho não faz avaliação de modelo de confiança, pois seu objetivo é analisar uma abordagem de divulgação do estado das chaves que serão utilizadas para fazer a verificação de um pacote de dados. Alguns métodos utilizados na Internet para validar chaves serão apresentados na próxima seção.

3. Revogação de certificados

Quando um pacote de dados faz referência a um indivíduo ou organização e o seu conteúdo é uma chave pública, ele essencialmente é um certificado digital [Jacobson et al. 2012]. Por isso, os termos "chave" e "certificado" serão utilizados de forma intercambiável no restante do artigo. Um certificado digital tem um período de validade durante o qual ele é confiável. Após seu período de validade, um certificado torna-se inválido e não é mais confiável. Durante o período de validade do certificado, o emissor do mesmo deve manter e fornecer informações sobre o estado do mesmo. O estado "revogado" indica que o período de validade do certificado foi prematuramente encerrado, portanto, não é mais confiável. Em PKI, uma Autoridade Certificadora (*Certification Authority* - CA) pode revogar um certificado por diversas razões, como: comprometimento da chave privada do titular; comprometimento da chave privada da autoridade certificadora, o que significa que todos os certificados emitidos pela mesma são potencialmente não-confiáveis e devem ser revogados; mudanças nas informações relativas ao titular do certificado; violação da política de segurança da autoridade certificadora pelo assinante; entre outras [Cooper et al. 2008].

3.1. Revogação de certificados na Internet

Na Internet convencional, uma CA deve manter e divulgar uma lista de revogação de certificados (*Certificate Revocation List* - CRL). Essa lista é uma estrutura de dados digitalmente assinada pela CA emissora dos mesmos, contendo a data e a hora de sua publicação, o nome da CA emissora e o número de série dos certificados revogados que ainda não expiraram. Para poder confiar em um certificado, a aplicação deve verificar se seu número de série não consta da lista de revogação de certificados. Para tal, vários métodos diferentes podem ser empregados. A lista de revogação de certificados pode ser consultada pela aplicação do usuário, acessando um repositório disponibilizado pela CA e fazendo o

[2]Infraestrutura de Chave Pública (*Public Key Infrastructure* - PKI) é um sistema de gerenciamento de chaves públicas especificado em [Cooper et al. 2008].

download da lista. A aplicação precisa saber quando a CA publicará uma nova lista para poder manter-se atualizada. Quando o titular de um certificado solicita uma revogação, ele deve aguardar até que a CA publique a próxima CRL. Toda CRL deve informar também a data e hora em que será publicada uma nova CRL. A CA poderá antecipar a sua atualização, porém nunca deverá atrasá-la [Cooper et al. 2008].

O protocolo OCSP (*Online Certificate Status Protocol*) [Santesson et al. 2013] foi proposto como uma solução alternativa às CRLs. Este protocolo permite que as aplicações possam consultar o estado de um certificado *online*. As consultas efetuadas ao serviço OCSP retornam menos informações que uma CRL, uma vez que ele só responde pelo certificado especificado na consulta, enquanto a CRL retorna uma lista que pode ter informações de mais de um certificado. Por outro lado, o cliente precisa se conectar ao serviço OCSP para realizar as consultas, enquanto a CRL funciona de forma *offline*.

CRL e OCSP são as principais abordagens para fornecer informações de certificados revogados, sendo utilizadas pela maioria das aplicações que dependem da utilização de certificados digitais. Algumas variantes destas soluções foram criadas, como o OCSP *Stapling*, que funciona como uma extensão do protocolo de comunicação segura TLS, para reduzir o consumo de recursos em sistemas com grande fluxo de usuários [Eastlake 3rd 2011]. Porém, essas variações são implementadas de acordo com a necessidade de cada aplicação. Podemos mencionar também que o Google anunciou planos para desativar completamente o OCSP no seu navegador *Chrome*. Ao invés do OCSP, ele irá reutilizar seu mecanismo de atualização de software existente para manter uma lista de certificados revogados em seus clientes [Topalovic et al. 2012].

3.2. Revogação de certificados em ICN

Devido ao processo de revogação estar associado ao gerenciamento de certificados, esse tema é pouco explorado em ICN de forma isolada. Alguns artigos que tratam do gerenciamento de confiança mencionam o processo de revogação de forma bem sucinta. [Zhang et al. 2011] propõem um sistema de gerenciamento de confiança utilizando criptografia baseada em identidade (*Identity-Based Cryptography* - IBC). Nessa proposta, os certificados são gerenciados por um sistema chamado PKG - *Private Key Generator*. Esse sistema não prevê revogação, uma vez que mensalmente as chaves privadas são atualizadas automaticamente.

[Yu 2015] define uma abordagem de distribuição de certificados com ênfase nos produtores de conteúdo, apresentando uma proposta de revogação de assinaturas. O autor menciona vários desafios da gestão de chaves públicas em NDN e propõe que os aplicativos utilizem um mecanismo independente de provisionamento de certificados. Sua proposta adota um sistema de provisionamento de certificados, eliminando a necessidade do publicador distribuir sua chave pública. Nesse trabalho, a revogação de uma chave é realizada através de uma *declaração negativa*, também chamada de *atestado de suicídio da chave*, que deve ser feita pelo proprietário da chave e adicionada a um repositório. O objetivo do autor não era o processo de revogação de certificados, pois ele propõe solucioná-lo através da revogação da assinatura com duas abordagens. A primeira delas é pedir ao dono da chave privada que publique uma declaração negativa sobre a assinatura, e a segunda é a de manter a publicação de uma declaração positiva até a assinatura ser revogada ou expirar.

Alguns métodos para rejeitar conteúdos assinados com chaves que foram comprometidas são analisados em [Mauri and Verticale 2013]. Um dos métodos, chamado de *proativo*, consiste na sincronização de repositórios de chaves. Os outros dois métodos são chamados de *reativos*, sendo que um deles é baseado em *timestamps*. Neste método, o requisitante envia um pacote de interesse solicitando uma chave, especificando um *timestamp* que indica o limite de validade. Quando um nó recebe o interesse, ele verifica se possui a chave e se seu *timestamp* é mais recente que o *timestamp* do interesse. Se a condição for satisfeita, o nó envia o pacote de dados correspondente que contém a chave. Caso contrário, o nó encaminha o interesse para o nó seguinte. Se nenhum nó tem a chave recente, o interesse é encaminhado até o detentor da chave original. O outro método reativo consiste em obter a chave diretamente do publicador, através de um parâmetro do pacote de interesse que indica que o dado deve ser obtido diretamente da sua fonte original. Os autores comparam o desempenho de obtenção das chaves em termos de atraso, taxa de transferência e taxa de acertos, e concluem que a solução baseada em *timestamps* oferece o melhor compromisso entre atraso e sobrecarga da distribuição do estado da chave.

3.3. Ataque aos conteúdos

Em NDN, a verificação da assinatura dos pacotes de dados permite identificar conteúdo falso, porém a verificação é opcional para os roteadores e obrigatória para os clientes. O fato dos roteadores não serem obrigados a verificar assinaturas os torna vulneráveis a diversos tipos de ataques aos conteúdos, entre eles um ataque chamado *envenenamento de conteúdo* [Gasti et al. 2013]. Nesse ataque, um atacante pode utilizar uma chave comprometida para assinar conteúdos falsos e distribuí-los na rede. Devido a essa situação, o processo de verificação do estado da chave torna-se de extrema importância para a validação dos conteúdos.

4. Serviço de consulta do estado de chaves

Com base nas abordagens apresentadas na Seção anterior, aqui é proposto um serviço de divulgação do estado de certificados em ICN inspirado no OCSP, porém adaptado para trabalhar nos moldes da ICN. Em ICN, conforme exposto anteriormente, o publicador de um conteúdo não precisa estar disponível para que o cliente possa recuperá-lo; essa característica é apropriada para o serviço aqui proposto. A publicação da revogação será feita de forma *online* e não periodicamente como na CRL tradicional.

O serviço de consulta proposto tem como objetivo fazer com que a informação do estado das chaves seja disponibilizada de forma rápida e segura para os clientes. Por se tratar de um serviço especializado, mecanismos de controle devem ser implementados para garantir a confiabilidade das informações fornecidas. Os controles implementados podem ser baseados no modelo de confiança proposta para NDN [Yu et al. 2015]. As ligações de confiança entre os publicadores, o serviço de consulta e a aplicação devem ser estabelecidas por esse modelo. A aplicação deve conter um conjunto de chaves necessárias para efetuar a validação das respostas emitidas pelo serviço de consulta.

A solução proposta tem como objetivo atender aplicações que possuem os certificados instalados junto com a aplicação e/ou aplicações que, após acessar o conteúdo de um determinado publicador, mantêm o certificado armazenado para utilização posterior. Para essas aplicações, a utilização de certificados digitais com tempo de vida curto causaria uma carga de trabalho adicional para obter novos certificados. Como elas fazem

uso do mesmo certificado com frequência, não seria necessário buscar um novo certificado toda vez que tiverem de validar um pacote de dados do mesmo publicador. Ao invés disto, basta consultar o estado da chave através do serviço de consulta proposto. O serviço deverá estar distribuído pela rede com intuito de reduzir o tempo de resposta e a melhorar disponibilidade da informação do estado das chaves, reduzindo a dependência de um único ponto de acesso.

O mecanismo de consulta avaliado é baseado no modelo de replicação passiva [Budhiraja et al. 1993], no qual um ou mais dos servidores atuam como coordenadores da replicação. A função dos coordenadores é receber as informações de estado dos certificados fornecidas pelo publicador e manter as réplicas atualizadas. As réplicas são responsáveis por responder as consultas solicitadas pelos clientes. Com o objetivo de melhorar a disponibilidade da solução, o serviço pode conter mais de um coordenador, conforme ilustrado na Figura 4.

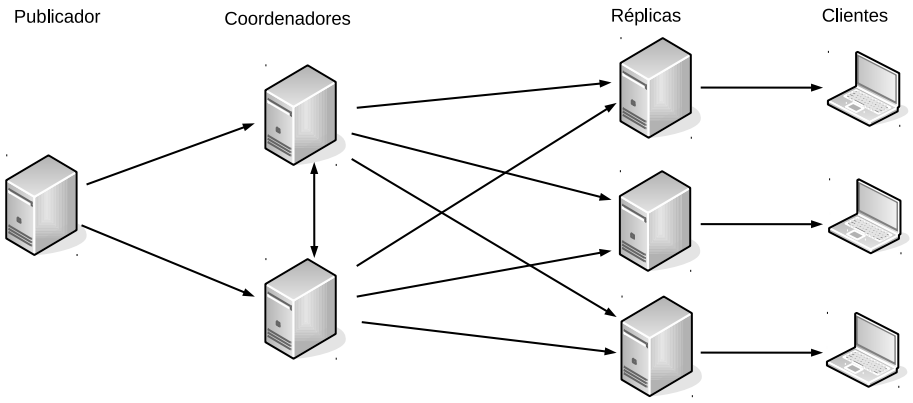


Figura 4. Arquitetura proposta.

As operações de atualização das réplicas sempre serão feitas por um único usuário (o responsável pelo certificado) para o mesmo registro. A atualização consiste em uma operação de escrita referente à inclusão de um novo registro ou à atualização de um registro existente. Devido a esse perfil operacional, não ocorrerão transações concorrentes para operações de escrita sobre o mesmo registro. A consistência dos dados no processo de escrita está garantida, não sendo necessário utilizar nenhum tipo de controle de concorrência ou de ordenação de eventos. As operações de leitura sempre retornarão um único registro. Por mais que a solução possa receber um pacote com várias consultas, elas serão processadas individualmente.

A Figura 5 ilustra o funcionamento geral do serviço proposto, que está dividido em: (i) o publicador do conteúdo, (ii) o serviço de consultas e (iii) a aplicação. Antes de servir o conteúdo para os clientes, primeiramente o publicador deve criar um par de chaves que serão utilizadas para assinar e validar os conteúdos. Após a sua geração, a chave que será utilizada para validação é agregada à aplicação (seta 1) e também enviada para o serviço de consulta (seta 2). A chave privada é armazenada de forma segura pelo publicador e será utilizada para assinar os conteúdos (setas 3 e 4). Quando os conteúdos são produzidos e assinados, os pacotes de dados deverão possuir a informação de qual chave é necessária para validá-los. Ao instalar a aplicação de acesso aos conteúdos (seta 5), o cliente possuirá as chaves necessárias para validar os conteúdos que serão obtidos

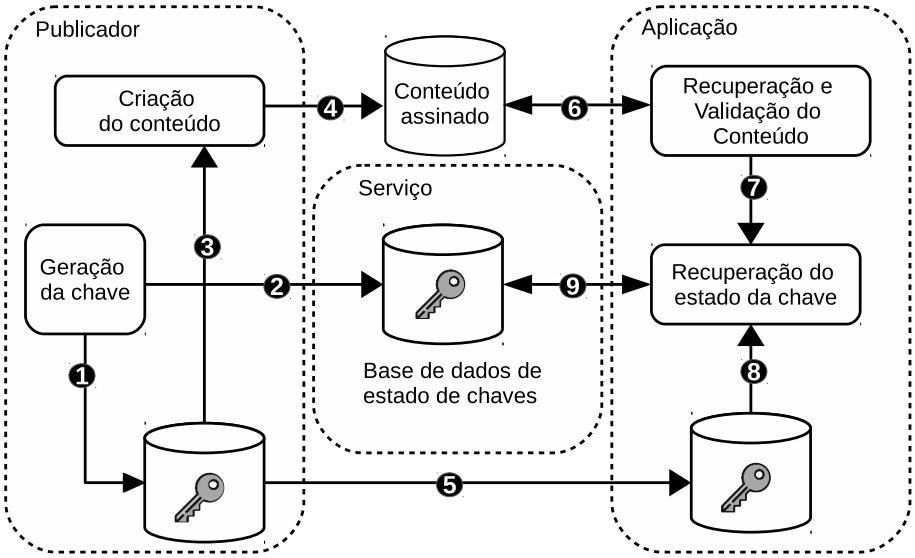


Figura 5. Funcionamento do serviço de consulta.

por ela. Quando o cliente obtiver um conteúdo (seta 6) para o qual ele já possui a chave para validá-lo (setas 7 e 8), basta apenas tentar obter a informação de estado da chave, fazendo uma solicitação ao serviço respondedor (seta 9).

A estrutura interna do serviço de consulta é ilustrada na Figura 6. Ao receber um pacote de interesse de consulta do estado de uma chave (seta 1), primeiramente esse pacote precisa ser validado com o objetivo de confirmar se o pacote esta utilizando as especificações do serviço. Após essa validação, uma consulta é efetuada na base de dados de informações de chaves (setas 2 e 3). A partir do resultado da consulta, um pacote de dados com a resposta é construído (seta 4), assinado pelo serviço respondedor (seta 5) e encaminhado de volta para a rede (seta 6).

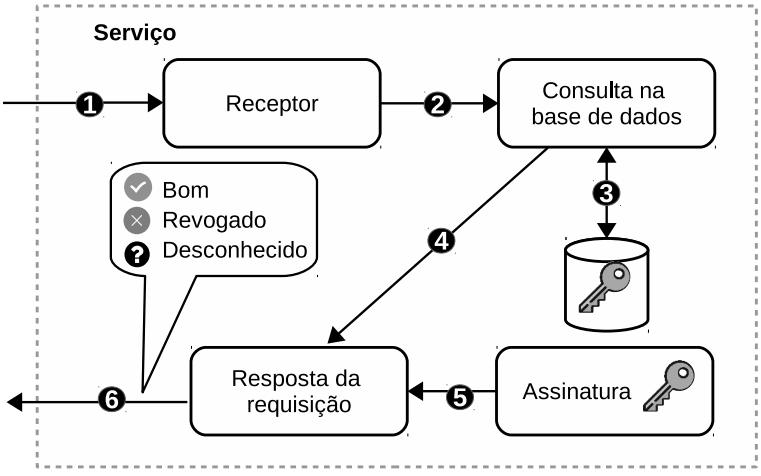


Figura 6. Estrutura interna do serviço.

5. Avaliação da proposta

Dada a indisponibilidade de uma plataforma ICN real para os experimentos, a proposta foi avaliada através de modelos de simulação. As simulações foram construídas utilizando o

módulo ndnSIM versão 2.3 do simulador NS-3 [Mastorakis et al. 2016] sobre a topologia RocketFuel [Spring et al. 2002] que possui características de grandes *backbones* reais. Foi utilizado o *template* NTT (AS2914) ilustrado na Figura 7, que é disponibilizado pelo simulador. O *template* possui 269 roteadores, 190 servidores e 461 clientes.

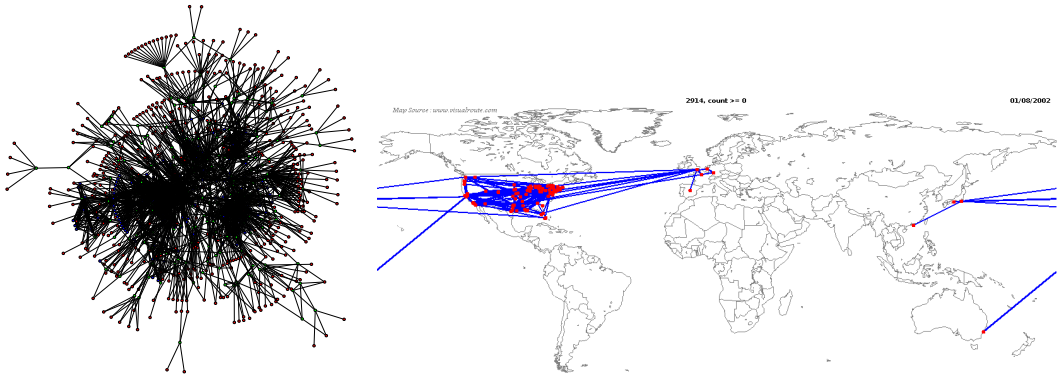


Figura 7. Topologia RocketFuel [Spring et al. 2002].

A métrica utilizada para avaliar o desempenho da solução proposta é o tempo de resposta das requisições dos clientes (t_r), ou seja, o tempo decorrido entre a requisição do estado de uma chave por um cliente (t_{req}, *request*) e a recepção da resposta correspondente (t_{rep}, *reply*). O tempo de resposta médio (t_m) corresponde à média dos tempos de resposta observados em todos os n clientes, ou seja:

$$t_m = \frac{\sum_1^n t_r(i)}{n} = \frac{\sum_1^n (t_{rep}(i) - t_{req}(i))}{n} \quad (1)$$

Os experimentos foram realizados com um número inicial de 25 clientes, sendo esse número duplicado sucessivamente até chegar a um total de 400 clientes. Inicialmente foram realizados experimentos sem a utilização de réplicas, ou seja, os clientes obtêm a informação do estado das chaves diretamente do publicador. Os demais experimentos foram realizados partindo de 5 réplicas, sendo esse número duplicado até total de 80 réplicas. Cada experimento com um mesmo conjunto de parâmetros foi executado 35 vezes. Em todos os experimentos, o maior coeficiente de variação observado foi de 9,5%, no cenário de 25 clientes. Já para o cenário com 400 clientes o coeficiente de variação máximo foi de 1,6%, o que demonstra uma boa estabilidade dos resultados com um número maior de clientes.

A Figura 8 apresenta os tempos de resposta médios observados nos experimentos. Para o serviço de consulta sem réplicas, o tempo médio de resposta com 25 clientes foi de 239,4 milissegundos, caindo para 169,8 milissegundos com 400 clientes. Ao adicionar as réplicas do serviço de consulta, o tempo médio diminuiu em todos os cenários. À medida em que mais clientes vão sendo adicionados, observa-se uma diminuição nos tempos médios de resposta. Esse efeito é previsível em NDN, pois mais requisições para o mesmo conteúdo são agregadas às tabelas de interesses pendentes dos roteadores.

A Tabela 1 detalha os percentuais de redução no tempo para obter o estado de um certificado em relação ao tempo de resposta sem réplicas do serviço de consulta. Com a

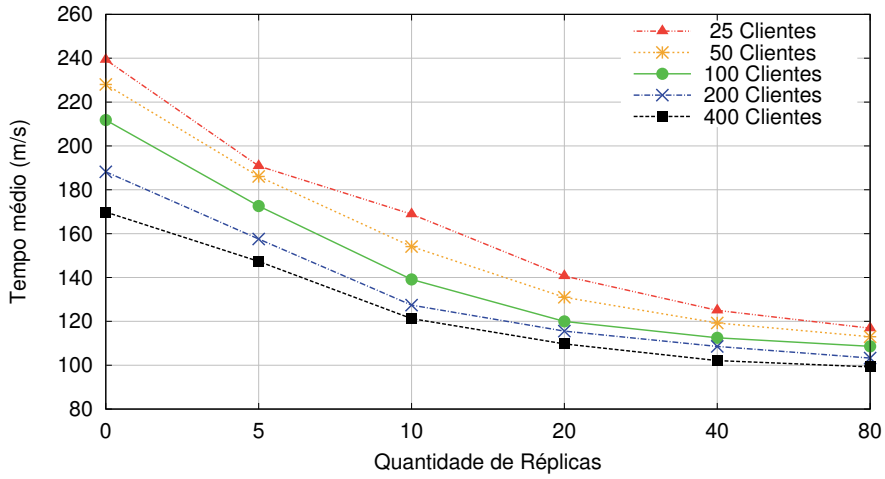


Figura 8. Tempos de resposta médios

adição de 5 réplicas o tempo de resposta para obter o estado de um certificado diminuiu em média de 13,2% a 21,3%, podendo atingir um ganho de até 53% com 80 réplicas. Observa-se em todos os cenários que os ganhos não são significativos a partir de uma certa quantidade de réplicas. Portanto, a partir de uma determinada quantidade de réplicas não é mais viável adicionar novas réplicas ao sistema. Por exemplo, no cenário com 400 clientes e 40 réplicas, a redução no tempo de resposta é de 39,8% e com 80 réplicas a redução passa a 41.5%, um ganho pequeno frente ao dobro de réplicas necessárias.

Tabela 1. Redução no tempo de resposta médio.

Clientes / Réplicas	25	50	100	200	400
5	21,3%	18,3%	18,5%	16,2%	13,2%
10	30,9%	32,4%	34,3%	32,2%	28,6%
20	43,2%	42,5%	43,3%	37,5%	35,3%
40	50,1%	47,7%	46,8%	42,3%	39,8%
80	53,7%	50,4%	48,7%	45,1%	41,5%

A Figura 9 apresenta o tempo mínimo, médio e máximo necessário para atualizar todas as réplicas com o novo estado de uma chave, em um cenário com 100 clientes. O valor mínimo é o tempo necessário para o coordenador receber a confirmação de que a primeira réplica foi atualizada; o valor máximo é o tempo decorrido até o coordenador receber a resposta da última réplica atualizada. Os resultados demonstram que a inclusão de mais réplicas não causa muita influência no tempo necessário para a atualização da informação em todas as réplicas na rede.

6. Conclusão e Trabalhos Futuros

Este artigo apresentou a proposta de um serviço de consulta do estado de chaves/certificados em redes ICN, inspirado no protocolo OCSP [Santesson et al. 2013]. Esse serviço é baseado em um esquema de replicação passiva, onde as réplicas são espalhadas pela rede e atendem as consultas dos clientes.

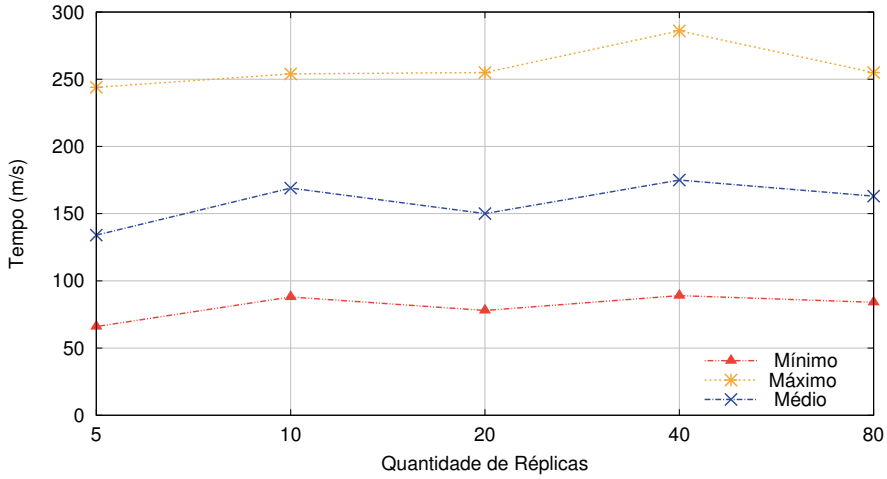


Figura 9. Tempo médio para atualização das réplicas.

O serviço de consulta proposto foi avaliado através de um modelo de simulação, usando o módulo ndnSIM do simulador NS-3 [Mastorakis et al. 2016] e o template NTT (AS2914) da topologia RocketFuel [Spring et al. 2002]. Os experimentos realizados demonstram que a arquitetura proposta foi eficiente na redução do tempo médio de obtenção da informação do estado das chaves pelos clientes. Através do serviço de consulta distribuído, os clientes conseguem obter o estado de um certificado de forma mais rápida. Todavia, observa-se que que após uma determinada quantidade de réplicas de consulta serem adicionadas, a inclusão de novas réplicas não gera ganhos significativos.

Como trabalhos futuros, devem ser realizados mais experimentos em diferentes topologias com quantidades maiores de clientes, e efetuar testes de disponibilidade do serviço de consulta no caso de falhas das réplicas.

Referências

Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and Ohlman, B. (2012). A survey of information-centric networking. *IEEE Communications Magazine*, 50(7):26–36.

Budhiraja, N., Marzullo, K., Schneider, F. B., and Toueg, S. (1993). The primary-backup approach. *Distributed systems*, 2:199–216.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W. (2008). Internet x.509 public key infrastructure certificate and certificate revocation list (CRL) profile. Technical report, ed.: RFC 5280, Internet Engineering Task Force (IETF).

Eastlake 3rd, D. (2011). Transport layer security (TLS) extensions: Extension definitions. Technical report, ed.: RFC 6066, Internet Engineering Task Force (IETF).

Gasti, P., Tsudik, G., Uzun, E., and Zhang, L. (2013). DoS and DDoS in named data networking. In *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*, pages 1–7. IEEE.

Ghodsi, A., Shenker, S., Koponen, T., Singla, A., Raghavan, B., and Wilcox, J. (2011). Information-centric networking: seeing the forest for the trees. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, page 1. ACM.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M., Briggs, N., and Braynard, R. (2012). Networking named content. *Commun. ACM*, 55(1):117–124.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., and Braynard, R. L. (2009). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 1–12. ACM.

Mannes, E., Maziero, C., Lassance, L. C., and Borges, F. (2016). Assessing the impact of cryptographic access control solutions on multimedia delivery in information-centric networks. In *Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP*, pages 427–435. IEEE.

Mastorakis, S., Afanasyev, A., Moiseenko, I., and Zhang, L. (2016). ndnSIM 2: An updated NDN simulator for NS-3. Technical report, Technical Report NDN-0028, Revision 2, NDN.

Mauri, G. and Verticale, G. (2013). Distributing key revocation status in named data networking. In *Meeting of the European Network of Universities and Companies in Information and Communication Engineering*, pages 310–313. Springer.

NDN (2014). NDN specification documentation. `http://named-data.net/wp-content/uploads/2013/11/packetformat.pdf`.

Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C. (2013). X. 509 internet public key infrastructure online certificate status protocol OCSP. Technical report, IEEE.

Spring, N., Mahajan, R., and Wetherall, D. (2002). Measuring ISP topologies with rocketfuel. *ACM SIGCOMM Computer Communication Review*, 32(4):133–145.

Topalovic, E., Saeta, B., Huang, L.-S., Jackson, C., and Boneh, D. (2012). Towards short-lived certificates. *Web 2.0 Security and Privacy*.

Yu, Y. (2015). Public key management in named data networking. Technical Report Tech. Rep. NDN-0029, NDN.

Yu, Y., Afanasyev, A., Clark, D., Jacobson, V., Zhang, L., et al. (2015). Schematizing trust in named data networking. In *Proceedings of the 2nd International Conference on Information-Centric Networking*, pages 177–186. ACM.

Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Crowley, P., Papadopoulos, C., Wang, L., Zhang, B., et al. (2014). Named data networking. *ACM SIGCOMM Computer Communication Review*, 44(3):66–73.

Zhang, X., Chang, K., Xiong, H., Wen, Y., Shi, G., and Wang, G. (2011). Towards name-based trust and security for content-centric network. In *2011 19th IEEE International Conference on Network Protocols*, pages 1–6. IEEE.

Impact of Multipath in Mobile Backhaul Savings for ICN Architectures: An Evaluation Using ndnSIM

Silvia Lins[1], Lian Araujo [1], Andrey Silva[1], Neiva Fonseca[2] and Aldebaro Klautau[1]

[1]LASSE - 5G and IoT Research Group
Universidade Federal do Pará (UFPA)
Belém – PA – Brazil

[2]Ericsson Research
Stockholm, Sweden

{silvialins, ivanes, andreysilva, aldebaro}@ufpa.br

neiva.lindqvist@ericsson.com

Abstract. *Current video streaming demands are motivating research on cost-efficient solutions for distributing such large traffic amount. Information-Centric Networking (ICN) is a relevant new paradigm that can inherently benefit from multipath transport. This work contributes specifically evaluating the impact of multipath transport in ICN deployments with and without cache, assessing its capacity to alleviate bottlenecks in the radio access network backhaul links. Previous related work has evaluated cache and multipath techniques jointly used, but in this work new insights are provided regarding how multipath functionality alone already impacts in a positive way ICN deployments. Another contribution of this work is evaluate cache deployment in various aggregation nodes in realistic mobile operator inspired scenario, showing how its location influences in end-to-end delay reduction. Evaluation is performed using the open source ndnSIM simulator and, e. g. , indicates that backhaul savings originated by multipath deployment are relevant even without cache, and also assesses cache deployment in intermediate aggregation nodes.*

1. Introduction

Mobile traffic is expected to grow 53 % from 2015 to 2020 [Cisco 2015]. To cope with this traffic growth, ICN architecture can empower content distribution and enhance network performance as much as end-user experience. Some studies [Yi et al. 2013] indicate that multipath, a concept that overlaps with network forwarding strategies, is a key enabler for the benefits provided by the ICN networks. Therefore, it would be relevant to evaluate multipath impact in mobile networks correlating it to the use of a specific forwarding scheme.

ICN considers a content, or a name, as the core of the Internet protocol stack, replacing the IP address field [Zhang et al. 2014]. This solution removes the anchor between information and host (maintained by the IP architecture since its beginning) performing content distribution in a much more efficient way, and deploying cache and multipath natively [de Brito et al. 2013]. Several cache studies were addressed in ICN literature, but optimized cache deployment is still far from being a trivial task [Yi et al. 2013]

due to its interplay with multipath and congestion control functions for example. It also depends on the network topology, traffic and several other aspects.

Such indications that gains related to the cache usage in ICN are also related to other ICN features, as well as network scenario characteristics, are present in some state of the art works, but they do not specify which functionality gives the most expressive contributions: According to [Imbrenda et al. 2014], caching a negligible amount of memory on customer premises reduces the load in the access network by 25%. In [Carofiglio et al. 2015], customized traffic measurements obtained from a mobile operator scenario implementing multipath, showed that traffic can be reduced from 60% to 95% during the peak hour by using few GBs of memory in network equipment. On the other hand, in [Fayazbakhsh et al. 2013] it is established that the optimistic best-case improvement that ICN can provide is 17% over the simple edge-caching architecture (considering all metrics). Such result variations indicate that studies indicating specific multipath benefits in ICN caching are still missing.

To the best of the authors' knowledge, ICN open literature does not inform, for example, a percentage of traffic reduction solely obtained with the addition of caching or multipath separately or if there are advantages in placing cache on intermediate (aggregation) nodes. Also, specific savings for the Mobile Backhaul (MBH) links, i.e. links near access connecting macro sites with the first aggregation point, are so far unclear. Such mobile backhaul link is "a potentially very damaging bottleneck if it lacks the required capacity" according to [Paolini 2011], and corresponds to approximately 30% of the total network operational costs [Skyfiber 2013].

Other relevant aspect in ICN architecture simulations is the choice of the simulation tool. Several open-source softwares are currently available, an ndnSIM [Mastorakis et al. 2015] is the most used among them [Tortelli et al. 2016]. In [Tortelli et al. 2016] it is stated that almost 2/3 of the presented results in the area are not reproducible because either the authors have not specified the tool used for evaluation (20%) or because they used a custom simulator (40%), which is the case of cache studies [Imbrenda et al. 2014] and [Carofiglio et al. 2015] aforementioned. In this respect, these studies are complemented here, where ndnSIM simulator was chosen to perform simulations and make this work results more easily checked. With a scenario inspired by a mobile operator topology implemented in a tree-like topology [Carofiglio et al. 2015], this paper evaluates and details the multipath impact and benefits in ICN cache deployments, showing which percentage of traffic reduction was solely obtained with multipath functionality addition and which was achieved by enabling cache in different network nodes. This paper also specifies the gains related to the macro sites backhaul link and assess the best cache location deployment options.

The next sections are organized as follows: in Section 2, the ICN paradigm is described and has its advantages and disadvantages contrasted with IP architectures. Section 3 details the multipath strategy adopted. In Section 4, the chosen simulation scenario is detailed, specifying the traffic models used as well as the simulation parameters. Section 5 presents and discusses the results. Section 6 concludes the work and provides the expected next steps in this research.

2. ICN Overview

ICN - Information Centric Networking [Xylomenos et al. 2014] is a proposal to deploy Internet architecture in a way that it removes the anchor between the content and the host imposed by IP. CCN (Content Centric Networking) [Jacobson et al. 2009] and NDN (Named Data Networking) [NDN 2014] are currently the main drivers in the ICN research area for ICN architectural deployment.

First CCN article was published in 2009 [Jacobson et al. 2009] and proposed an architecture that could allegedly achieve performance and security while easily scale, when compared to IP. As already mentioned, IP architecture is currently making use of several add-ons that increase network topology cost and complexity, like CDN servers and middle-boxes. NDN proposes changing the IP field to a content field, which is very adjustable and can even be layered over IP itself for compatibility purposes.

Information exchange in CCN/NDN architectures comprises two main structures: data packets and interest packets. Both packet structures carry a name that identifies the content, and the communication is mainly operated by the receiver node, or "consumer".

The process happens as follows: The consumer inserts the name that identifies the content or information piece it wants to retrieve from the network inside an interest packet and sends to the network. After forwarding the interest, consumer defines a timer to wait for a response from the network. If nothing is received, it resends the interest and resets the timer. The network node receiving the interest first performs a search in its "content store" (CS), i.e. a content cache. If found, the content is directly sent back to the node or interface that requested it.

If the content is not found, the router checks the "Pending Interest Table", PIT, which is responsible to record the interfaces from which interest requests were received. If an existing entry is found in the PIT for the same content packet, the router just stores this new interface request referent to the same packet. Each Interest that arrives has also an associated lifetime. If it expires, the PIT entry is removed. If no entry is found in the PIT related to this content, the router records in the PIT this new entry associating interest request and interface and forwards this interest request to another router through the "Forwarding Information base" (FIB) structure. FIB records output interfaces (maybe multiple) for content packets. The interest is forwarded to each recorded output interface that may reply with the content packet.

This process is repeated until a node with the requested content is found. The content is sent back through the same path used to forward the corresponding interest, until it reaches the consumer (or the consumers) that requested the content.

Since NDN benefits from an adaptive forwarding plane, its various forwarding strategies allow measurement of QoS metrics and can change content routes according to congestion status for example. The concept of forwarding strategies frequently overlaps with the definition of multipath [Yi et al. 2013], and it is relevant to discuss the different forwarding strategies currently available for NDN networks.

3. NDN Forwarding Strategies

Forwarding in NDN is said to be adaptive because in the beginning, routers just define the interfaces available to send interests and their preference or priority of use, but this

information will be updated as soon as the network starts sending and receiving packets. Based on interface providing smaller average RTT statistics for example, FIB helps adapting interface preferences. The metric used for interface preference ranking depends on the chosen forwarding policy, which acts according to the information stored in FIB structures. Forwarding strategies can be used also to avoid congestion for example when imposing limits at the amount of Interests that can be forwarded per face.

Each NDN forwarding scheme might be more suitable for a certain application, e.g., Dynamic Adaptive S treaming [Rainer et al. 2016] or Quality of Service in general [Kerrouche et al. 2016].

Besides the schemes above, several forwarding strategies were already proposed for ICN networks [Li et al. 2016]. Among them, in this work a Pending Interest (PI) scheme was used, based on [Carofiglio et al. 2013], for its relevance and use in previous works [Carofiglio et al. 2015], [Nguyen et al. 2015]. For this strategy, considering a given router, when an interest packet must be forwarded, for each face n listed in its FIB for the according prefix, there is a weight w_n associated with it, defined as:

$$w_n = 1/P_n \tag{1}$$

where P_n is the number of pending interests for face n. The final resolution of which face will be used to forward an interest will be made probabilistically, according to the weight of each face. This multipath feature was not ready available in the simulator and was implemented in ndnSIM. The algorithm was mainly implemented in the ndnSIM Forwarding Strategy block. If more information from the algorithm implementation is needed, reference [Carofiglio et al. 2013] should be consulted.

In summary, forwarding strategies and multipath concepts are interdependent, and understanding one of them implies understanding the other as well. This work evaluates the multipath gains isolated and together with cache located in different network nodes. Section 4 will provide further details regarding the scenarios implemented in ndnSIM simulator.

4. Scenarios Description

Targeting performance evaluation of NDN architecture in the presence of multipath and cache functionalities, some specific scenarios were implemented using the ndnSIM simulator. All scenarios are based on a tree-like topology [**?**] [**?**], inspired by a real mobile operator deployment defined in [Carofiglio et al. 2015] and shown in Figure 1(a).

4.1. Baseline Scenario

Baseline cenario comprises 20 UEs (User Equipments) per macro site, being five macro sites in total. Links capacities between routers are defined as shown in Figure 1(a), and are also summarized in Table 1: Wireless links between UEs and macro sites have 1 Gbps while macro sites backhaul links (i.e. links that interconnect the base stations to the L3 routers) provide 400 Mbps. Connections between Level3 and Level2 routers are 500 Mbps links, connections between Level2 and Level1 routers are 1 Gbps links, connections between PGW and L1 are 2 Gbps links and the link interconnecting PGW to the content server provides 30 Gbps of bandwidth. This baseline is used as a reference

for all simulation setups, and does not consider cache existence neither multipath implementation, since multipath routing in IP access networks is not yet widely deployed in practice [Gurtov and Polishchuk 2009]. OSPF is used in this IP baseline scenario as the default routing protocol.

Table 1. Simulation Parameters: Link Capacities

Connection	Capacity
UE – Macro sites	1 Gbps
Macro sites – Level3 Routers	400 Mbps
Level3 Routers – Level2 Routers	500 Mbps
Level2 Routers – Level1 Routers	1 Gbps
Level1 Routers – PGW	2 Gbps
PGW – Content Server	30 Gbps

The baseline scenario has two flavors:

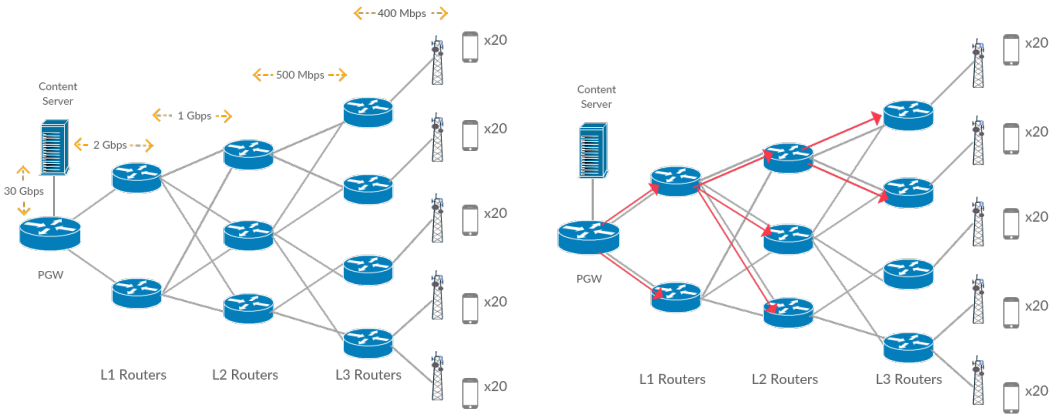
- It is modeled first as an IP-Based network, using ns-3 simulator, and does not implement cache neither multipath functionalities. It does not include any ICN property, and targets content distribution from the server to the UEs. It will be referred throughout this work as the "CDN" scenario, and was simulated to be used as a reference for end-to-end delay and throughput performance comparison with ICN scenarios. All results comparison are discussed in Section 5.
- It is also modeled as an ICN baseline scenario using ndnSIM, with all ICN properties described in Section 2. To generate several simulation scenarios in order to provide the desired comparisons, this ICN setup will be used as a base for other implementations as described in the sequel.

The following scenarios are derived implementations that take into consideration the ICN baseline provided above. They do not change links capacities configuration or network nodes location, only differing from one to another regarding the strategy adopted for cache placement and the existence or not of multipath features.

4.2. Multipath evaluation without cache deployment

First simulation comparison setup (Scenario 1) implements multipath functionality in the baseline provided by Section 4.1. In Scenario 1, nodes do not perform cache and multipath is enabled, implemented as described in Section 3. Obviously, only nodes that have two or more connections are able to use multiple paths to send and receive information, which according to Figure 1(a) excludes base station nodes, which have only one backhaul connection, and the content server. PGW use both links to forward packets to L1 routers and L1 routers also divide output traffic among the three links that interconnect them to the Level2 routers. Level2 routers are able to do the same with the links that connect them to the L3 routers. As already mentioned, the multipath adopted to distribute the traffic among the available interfaces for each router is detailed in Section 3 and is also depicted in red for better visualization in Figure 1(b).

Scenario 1 performance will be further compared in Section 5 with the ICN Baseline, without cache or multipath funcionalities (i.e. an ICN singlepath scenario), and these



(a) Baseline scenario implemented in ns-3 and in ndnSIM, inspired in a real mobile network deployment.

(b) Scenario 1: multipath implemented in ndnSIM, for all routers with two or more connections.

Figure 1. Baseline scenario and multipath scenario implemented for simulations.

results are also contrasted with the CDN baseline, which is IP-Based. These comparisons will enable assessment of multipath gains independently from cache advantages.

To evaluate cache gains in ICN deployments, two other scenarios were derived from the ICN baseline provided in 4.1: cache deployment without multipath (4.3), and cache deployment with multipath enabled(4.4).

4.3. Cache strategy evaluation: without multipath

Regarding cache placement evaluation, Scenario 2 is implemented considering only the existence of cache, without enabling multipath. Scenario 2 is further classified in four setups, each one deploying cache in different nodes. The same amount of cache is used in all scenarios, which corresponds to 1% of total content available for download [Li et al. 2012], as explained in the sequel:

- **Scenario 2.1:** In this setup, all cache is placed in the PGW node.
- **Scenario 2.2:** Cache is placed in R1 nodes only, divided equally among the L1 routers.
- **Scenario 2.3:** All cache placed in base station nodes, divided equally among them.
- **Scenario 2.4:** Cache is distributed in the nodes as follows: like in other cache scenarios, 1% of cache is assumed in the network. From this 1%, 4x more cache is placed in R3 and R4 nodes (i.e. 20000 packets), divided equally among levels and router nodes (10000 packets in L3, being 2500 packets per R3 router, and 10000 packets in base stations level, with 2000 packets per base station).

These setups were implemented to have its results contrasted with each other, evaluating what is the optimal cache placement setup for the targeted scenario. Its end-to-end delay and throughput statistics are also compared with the CDN baseline scenario, assessing how cache placement can impact positively backhaul bandwidth savings, as well as application latency. All setup for scenarios 2 are summarized in Figure 2.

4.4. Cache strategy evaluation: with multipath

The same scenarios setup from Section 4.3 were modeled with multipath activated, targeting the evaluation of cache and multipath functionalities jointly. Let's call scenarios

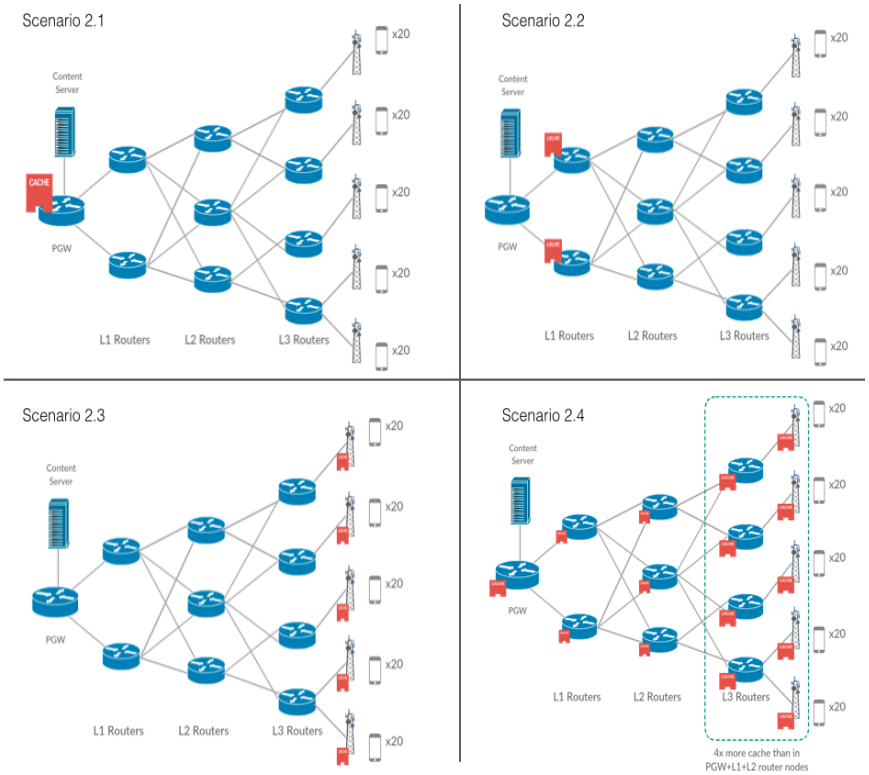


Figure 2. Scenario 2: Scenario designed for cache evaluation purposes, without multipath. Four different cache setups were implemented in ndnSIM.

for cache strategy evaluation with multipath as Scenario 3. They are shown in Figure 3 and its derived setups will be:

- **Scenario 3.1:** In this setup, all cache is placed in the PGW node, with multipath activated.
- **Scenario 3.2:** Multipath is also activated for this scenario, where cache is placed in R1 nodes only, divided equally among the L1 routers.
- **Scenario 3.3:** All cache placed in base station nodes, divided equally among them. Multipath is also enabled (for nodes with two or more connections, as expected).
- **Scenario 3.4:** Cache is distributed in the nodes as follows: like in other cache scenarios, 1% of cache is assumed in the network. From this 1%, 4x more cache is placed in R3 and R4 nodes (i.e. 20000 packets), divided equally among levels and router nodes (10000 packets in L3, being 2500 packets per R3 router, and 10000 packets in base stations level, with 2000 packets per base station). Multipath is also active for all nodes with multiple connections.

In total, 11 simulation runs are performed to compare different cache and multipath setups and isolate the gains associated with each one of them. First, ICN (singlepath) without cache and CDN/IP scenarios are compared (ICN Baseline vs. CDN/IP Baseline). Then, multipath is activated (Scenario 1) and compared with ICN Baseline. Next, Scenario 2 and Scenario 3 with different cache placements are simulated, and have its results compared with each other.

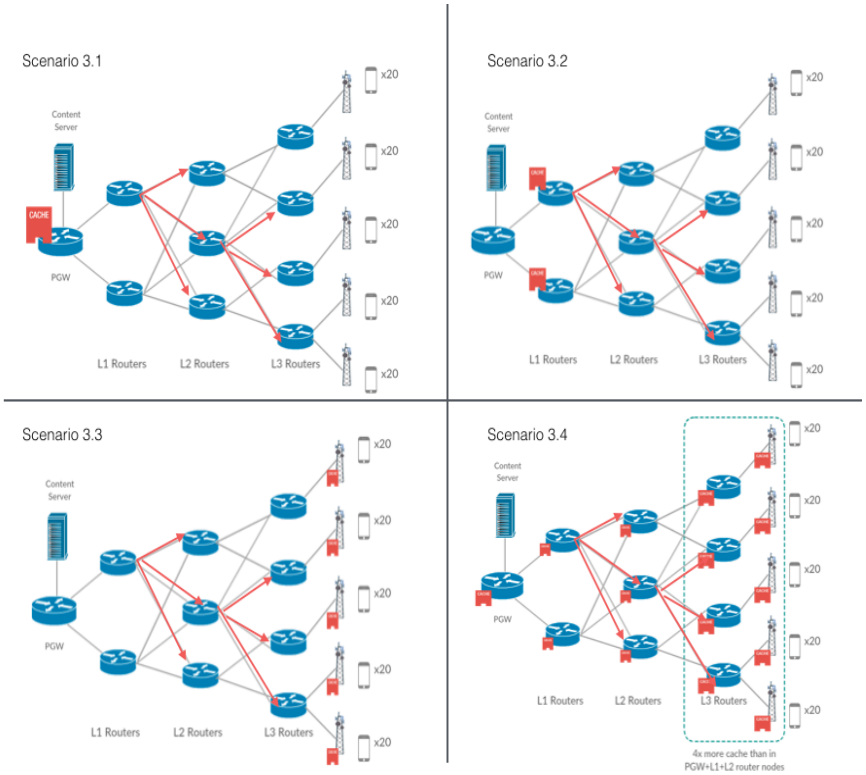


Figure 3. Scenario 3: Scenario designed for cache evaluation purposes, with multipath. Four different cache setups with multipath enabled were implemented in ndnSIM.

4.5. Traffic Modeling

Users demand traffic from the content server, which provides a variety of 10,000 contents each. 250 chunks of 4096 bytes compose each content, and users request contents according to an exponential distribution with a mean of 0.08 contents/s. Content popularity is modeled as a Weibull distribution with shape 0.8 and scale 500, as proposed by [Imbrenda et al. 2014]. For a given time T between two contents, users will request content chunks in a rate of 250/T chunks per second. In all scenarios, cache replacement policy adopted for the scenarios containing cache is LRU (Least Recently Used) [O'neil et al. 1993]. All simulation parameters are summarized in Table I.

Such traffic model assume that users are constantly retrieving content from the servers rather than sending information, which mimics current behavior for streaming applications for example. Results for the described simulation setups are discussed in the following section.

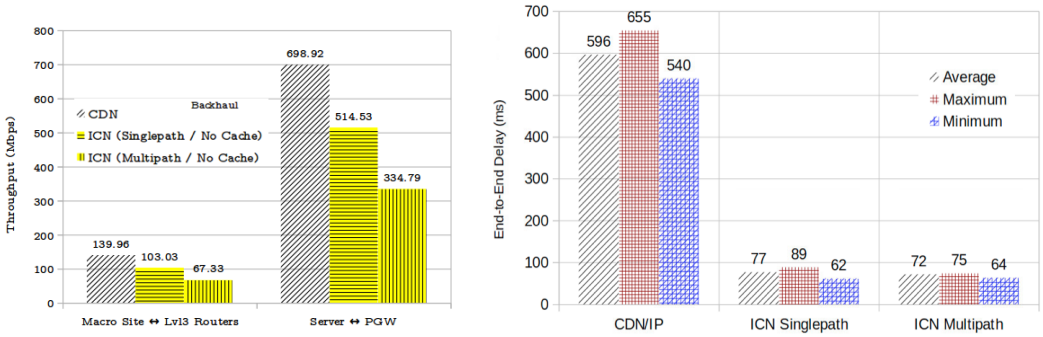
5. Results

First, the CDN/IP baseline scenario is simulated with the parameters provided by Section 4. In this scenario, multipath is not natively deployed and end-to-end connections are established between the server and UEs to send and receive information. Simulation results are compared with the ones from the ICN baseline scenario, which still does not assume multipath functionality but implements the information-centric paradigm for content distribution, as explained in Section 2. Multipath is then activated for the ICN sce-

Table 2. Simulation Parameters: Traffic Modelling

Parameter	Value
Contents per CDN server	10000
Active users per base station	20
Base stations per scenario	5
Chunks per content	250
Chunk size (Bytes) (%)	4096
Users content request rate modeling	Exponential distribution with mean of 0.8 contents/sec
Content size (KB)	1024
Content amount requested per UE in total	100 contents
Cache replacement policy	LRU
Content Popularity modeling	Weibull distribution (shape = 0.8, scale = 500)

nario and its results are contrasted with the ones obtained in both IP and ICN baselines, as shown in Figure 4(a).



(a) Macro site and PGW backhaul throughput in CDN/IP vs. ICN.

(b) Average, maximum and minimum end-to-end delay statistics in CDN/IP vs ICN Singlepath and ICN Multipath scenarios (without cache).

Figure 4. CDN vs. IP scenarios: Throughput and End-to-End delay results.

Results in Figure 4(a) evaluate multipath influence in backhaul traffic reduction. It assesses how backhaul savings can be correlated with multipath activation even in ICN scenarios without any cache, and how it compares with an IP-Based (CDN) scenario that does not implement cache neither multipath. As already stated, cache is not considered here because the intention is to isolate multipath gains and evalulate if they alone are worthy, and for the CDN scenario multipath is not present at all since it is not a native neither trivial function specially for IP-based networks.

First result observed from Figure 4(a) indicates that ICN itself without multipath (singlepath case) already provides around 26% of savings in Macro Site backhaul throughput (103 Mbps in the singlepath scenario against 139.96 Mbps in the CDN/IP scenario). This is due to the content dissemination paradigm adopted by ICN, where there is no need to establish several unique end-to-end connections between UEs and the server as

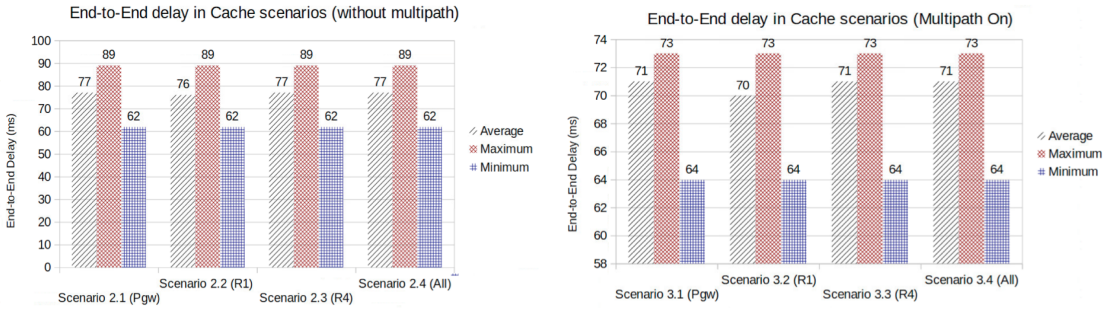
IP does. Interests for the same content sent by different users are updated in the pending interest table located in the router (and/or macro site) nodes and when the content arrives in the node, it is only copied and forwarded to the different outgoing ports (or users) that requested the same interest/content.

This positive impact is also reflected in end-to-end delay statistics shown in Figure 4(b). Even without cache, in both CDN and ICN scenarios the content popularity is modeled as a Weibull distribution as explained in Section 4.5. It allows (for the ICN paradigm) interest packet aggregation, which reduces delay specially in popular content requests.

Imagine a user A sending an Interest for a content P. Considering P as a popular content, users B, C and D also request P, before it arrives in A. In ICN scenarios, as soon as intermediate nodes identify several interests for the same content, they forward to the content server only the first request, from A, recording B, C and D as interfaces to forward the content as soon as it comes back from the server. By reducing server load as well as intermediate link demands, ICN scenarios avoid congestion occurance and also reduce end-to-end delay statistics specially for nodes B, C and D, since when they send requests for the same content, P was already in its way back from the server (because user A sent the request before).

In Figure 4(b), average end-to-end delay for the ICN scenarios stayed around 75 ms, while in CDN/IP scenarios it achieved almost 600 ms. It represents a delay reduction close to 87% for both singlepath and multipath scenarios, showing that even without investing in cache deployment ICN could be a good alternative for time-sensitive applications.

Considering cache location in ICN scenarios, different cache locations were simulated as detailed in Section 4.3. First, cache evaluation was performed without multipath functionality, running Scenarios 2.1 to 2.4 and comparing its end-to-end delay statistics. For the singlepath scenarios, Figure 5(a) shows that there was not considerable difference among the obtained results, only a slight advantage of 1 ms average delay reduction when placing cache in R1 nodes (Scenario 2.2). As already mentioned in Section 4.3, it is worth noticing that the same amount of cache was simulated in all scenarios, changing only the nodes in which cache was inserted.



(a) End-to-end delay statistics in ICN *singlepath* scenarios with the same amount of cache placed in different nodes.

(b) End-to-end delay statistics in ICN *multipath* scenarios with the same amount of cache placed in different nodes.

Figure 5. ICN Singlepath vs. ICN Multipath: End-to-End delay results.

Regarding multipath simulations, Figure 5(b) also shows that no relevant advantage was obtained by changing cache location in simulated scenarios 3.1 to 3.4 (only 1 ms reduction in average end-to-end delay for scenario 3.2). When contrasting singlepath versus multipath scenarios with cache activated, in Figure 6 reveals that around 8% of latency can be saved when placing cache in R1 level nodes (i.e. a reduction from 76 ms to 70 ms in average).

But going back to the results in Figure 4(b), it is clear that most of the gains are provided by the multipath activation only. Only 2 ms reduction could be assigned to the cache usage, since 72 ms average delay is already obtained by multipath activation only, depicted in Figure 4(b), and when activating cache in R1, Figure 6 shows that it only reduces to 70 ms.

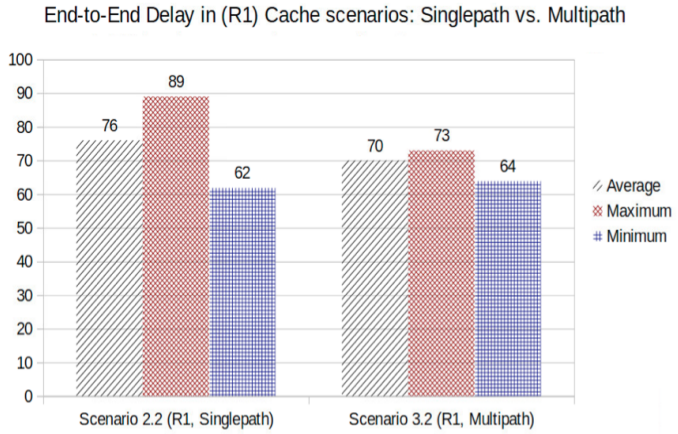
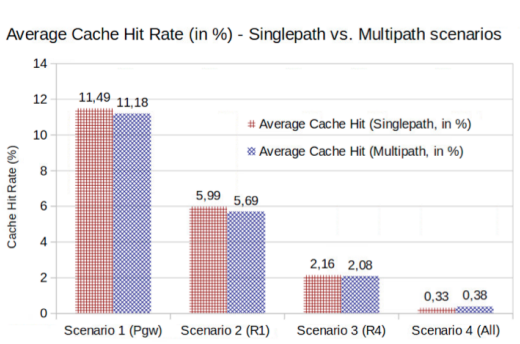


Figure 6. Average, maximum and minimum end-to-end delay statistics in ICN cache scenarios 2.2 and 3.2 (cache in R1 nodes), showing singlepath vs. multipath statistics.

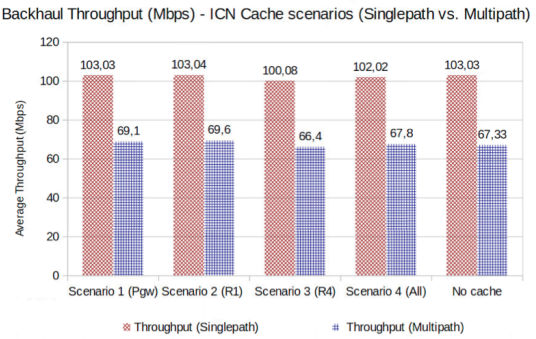
Cache hit rate statistics are able to confirm that multipath has a much more relevant role in end-to-end delay reduction than cache location. Figure 7(a) reveals that even placing all cache in PGW node (Scenarios 2.1 and 3.1), for both singlepath and multipath simulations only 11% of cache hit rate was obtained. When spreading cache among all router levels, less than 1% of cache hit was obtained, and when concentrating it in base stations (Scenario 3, cache in R4) only 2% of cache was used to respond to users requests.

Other previous cache studies [Carofiglio et al. 2015] showed more positive impact of cache and multipath functionalities in ICN scenarios, but the amount of cache used in these studies was considerably high when compared to total network available content: In [Carofiglio et al. 2015], 20,000 contents are available for retrieval by the users, and each content is divided in 250 chunks of 4096 bytes each, representing approximately a total of 20 GB. The authors in [Carofiglio et al. 2015] assumed 6 GB of cache, i.e. 30% of the total available content. This value can be considered large, given the current dimension of Internet. Here, the cache size represents only 1% of the amount of content available for retrieval, as suggested by other study [Li et al. 2012]. This allows to infer about the impact of this assumption.

Throughput statistics also reveal the relevance of multipath functionality in bandwidth savings when compared to cache addition. When placing all cache amount in



(a) Cache hit rate results for all singlepath and multipath scenarios.



(b) Average backhaul throughput results (connections between R3 nodes and Base Stations (R4)) for all singlepath and multipath scenarios.

Figure 7. Cache hit rate and backhaul throughput results for all singlepath and multipath scenarios.

R4 (base station) nodes, backhaul throughput demands around 66 Mbps if multipath is activated, contrasting with more than 100 Mbps if only singlepath is enabled. But a close enough result was already obtained when simulating ICN scenarios with multipath only, without any cache addition, as already showed in Figure 4(a) and also depicted in Figure 7(b). In brief, singlepath ICN scenarios demand around 100 Mbps in backhaul throughput, while multipath scenarios (without cache) demand 67 Mbps. It already represents a reduction of 34% in backhaul bandwidth demands, and when activating cache (if multipath is already active) it only helps saving 1 Mbps more in the best case (reducing from 67.33 Mbps in ICN multipath without cache scenario to 66.4 Mbps in ICN multipath with cache in base stations - Scenario 3.3.)

6. Conclusions and Next Steps

This paper evaluated through ndnSIM network simulations how multipath functionality itself could provide, even without any cache deployment, considerable backhaul savings in information centric networks. Gains were assessed regarding macro site backhaul savings as well as bandwidth usage reduction in backhaul network links and end-to-end delay statistics. Cache hit rate was also contrasted among different cache deployments in ICN scenarios. The first results compared ICN scenarios without cache, with and without multipath functionality, with a CDN/IP-based network containing the same traffic demands and topology (and also without cache).

Results of such comparison revealed that, regarding backhaul demand savings, the ICN content distribution paradigm even without multipath already provides savings around 26% in macro sites throughput and in PGW backhaul when compared to CDN architectures. But the main focus here is to conclude that considering an ICN with multipath deployment, without any cache addition, savings for the observed scenarios are already valuable when compared to ICN singlepath and even more with CDN/IP-Based, increasing gains to 52% in the macro site backhaul and 48% in the PGW backhaul when compared to CDN.

Regarding cache location, results indicated that if realistic cache amounts (i.e. 1% of total available content [Li et al. 2012]) are used, cache impact in both end-to-end delay

and backhaul throughput reduction is not relevant when compared to multipath benefits. A relevant aspect that is not tackled here and figures as future work is to evaluate multipath algorithms efficiency and computational costs, in order to provide a feasible realistic solution. Another open issue is to analyze the same aspects in congested networks, but it requires a congestion control algorithm for ICN, which is currently an open research question [Chai et al. 2013].

Another relevant aspect to be considered in future works is traffic modeling adaptation for next decade trends. So far, traffic modeling standards considers that the traffic from the network towards the user is still much larger than the traffic in the opposite direction, i.e. the uplink. As mentioned, the main objective with the simulations is to assess gains specific related to multipath functionality, and also to evaluate the advantages related to backhaul savings by doing cache deployment in different aggregation nodes. but future trends indicate that this behavior may change since users are already uploading more than 350 millions of photos per day on Facebook. Future mobile network trends where users also upload lots of contents (rather than only consuming content from the network) are also predicted by [Cisco 2015]. This change in user behavior will probably impact the cache strategies and other assessments with updated traffic models certainly will be needed.

References

Carofiglio, G., Gallo, M., Muscariello, L., Papalini, M., and Wang, S. (2013). Optimal multipath congestion control and request forwarding in information-centric networks. In *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, pages 1–10. IEEE.

Carofiglio, G., Gallo, M., Muscariello, L., and Perino, D. (2015). Scalable mobile backhauling via information-centric networking. In *Local and Metropolitan Area Networks (LANMAN), 2015 IEEE International Workshop on*, pages 1–6. IEEE.

Chai, W. K., He, D., Psaras, I., and Pavlou, G. (2013). Cache "less for more" in information-centric networks (extended version). *Computer Communications*, 36(7):758–770.

Cisco, V. N. I. (2015). Forecast and methodology, 2014-2019 white paper. *Technical Report, Cisco, Tech. Rep.*

de Brito, G. M., Velloso, P. B., and Moraes, I. M. (2013). *Information Centric Networks: A New Paradigm for the Internet*. John Wiley & Sons.

Fayazbakhsh, S. K., Lin, Y., Tootoonchian, A., Ghodsi, A., Koponen, T., Maggs, B., Ng, K. C., Sekar, V., and Shenker, S. (2013). Less pain, most of the gain: Incrementally deployable icn. In *ACM SIGCOMM Computer Communication Review*, volume 43, pages 147–158. ACM.

Gurtov, A. and Polishchuk, T. (2009). Secure multipath transport for legacy internet applications. In *2009 Sixth International Conference on Broadband Communications, Networks, and Systems*, pages 1–8.

Imbrenda, C., Muscariello, L., and Rossi, D. (2014). Analyzing cacheable traffic in isp access networks for micro cdn applications via content-centric networking. In *Pro-*

ceedings of the 1st international conference on Information-centric networking, pages 57–66. ACM.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., and Braynard, R. L. (2009). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 1–12. ACM.

Kerrouche, A., Senouci, M. R., and Mellouk, A. (2016). QoS-FS: A new forwarding strategy with QoS for routing in Named Data Networking. In *Communications (ICC), 2016 IEEE International Conference on*, pages 1–7. IEEE.

Li, J., Wu, H., Liu, B., and Lu, J. (2012). Effective caching schemes for minimizing inter-ISP traffic in named data networking. In *Parallel and Distributed Systems (ICPADS), 2012 IEEE 18th International Conference on*, pages 580–587. IEEE.

Li, M., Lukyanenko, A., Ou, Z., Yla-Jaaski, A., Tarkoma, S., Coudron, M., and Secci, S. (2016). Multipath transmission for the internet: A survey. *IEEE Communications Surveys Tutorials, vol. PP*, (99):1–41.

Mastorakis, S., Afanasyev, A., Moiseenko, I., and Zhang, L. (2015). ndnSIM 2.0: A new version of the NDN simulator for NS-3. *NDN, Technical Report NDN-0028*.

NDN (2014). NSF Named Data Networking project. Available: http://www.named-data.net/ Last accessed: December 2016.

Nguyen, D., Fukushima, M., Sugiyama, K., and Tagami, A. (2015). Efficient multipath forwarding and congestion control without route-labeling in ccn. In *Communication Workshop (ICCW), 2015 IEEE International Conference on*, pages 1533–1538. IEEE.

O'neil, E. J., O'neil, P. E., and Weikum, G. (1993). The LRU-K page replacement algorithm for database disk buffering. *ACM SIGMOD Record*, 22(2):297–306.

Paolini, M. (2011). An analysis of the total cost of ownership of point-to-point, point-to-multipoint, and fibre options. *White paper on crucial economics for mobile data backhaul*.

Rainer, B., Posch, D., and Hellwagner, H. (2016). Investigating the performance of pull-based dynamic adaptive streaming in NDN. *IEEE Journal on Selected Areas in Communications*, 34(8):2130–2140.

Skyfiber (2013). Breaking the Backhaul Bottleneck: Road to Profitable Backhaul. *Technical Report*.

Tortelli, M., Rossi, D., Boggia, G., and Grieco, L. A. (2016). ICN software tools: survey and cross-comparison. *Simulation Modelling Practice and Theory*, 63:23–46.

Xylomenos, G., Ververidis, C. N., Siris, V. A., Fotiou, N., Tsilopoulos, C., Vasilakos, X., Katsaros, K. V., and Polyzos, G. C. (2014). A survey of information-centric networking research. *IEEE Communications Surveys & Tutorials*, 16(2):1024–1049.

Yi, C., Afanasyev, A., Moiseenko, I., Wang, L., Zhang, B., and Zhang, L. (2013). A case for stateful forwarding plane. *Computer Communications*, 36(7):779–791.

Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Crowley, P., Papadopoulos, C., Wang, L., and Zhang, B. (2014). Named data networking. *ACM SIGCOMM Computer Communication Review*, 44(3):66–73.

Uma aplicação de troca de arquivos em redes oportunistas

André F. Martins, Carlos A. V. Campos

Programa de Pós-graduação em Informática - PPGI
Universidade Federal do Estado do Rio de Janeiro – UNIRIO

{andre.martins,beto}@uniriotec.br

Abstract. *Opportunistic network is a paradigm that emerged from the mobile ad hoc networks, in which the node mobility offers opportunities for data transfer. It is a completely challenging networking model in which distributed applications will have to be modified to work. In this paper, we discuss the main features that a data application must have to function opportunistically. Furthermore, we propose an application for file exchange, by which show that certain modifications in P2P applications benefit the dissemination of file parts, decreasing the time required to achieve complete copy by reducing the number of hops without assistance from any infrastructure. Through the performance evaluation conducted by simulation, the proposed application was demonstrated promising to exchange files in opportunistic context.*

Resumo. *Rede oportunista é um paradigma que emergiu das redes móveis ad hoc, em que a mobilidade dos nós oferece oportunidades para a transferência de dados. É um modelo inteiramente desafiador de redes no qual as aplicações distribuídas terão que sofrer modificações para funcionarem. Neste artigo, discutiremos as principais características que uma aplicação de dados deve ter para funcionar de maneira oportunista. Além disso, proporemos uma aplicação para troca de arquivos, pela qual mostramos que determinadas modificações introduzidas em aplicações do tipo par-a-par (P2P) favorecem a disseminação das partes do arquivo, diminuindo o tempo necessário para se conseguir a cópia completa através da redução do número de saltos sem auxílio de qualquer infraestrutura. Através da avaliação de desempenho realizada por simulação, a aplicação proposta se demonstrou promissora para a troca de arquivos no contexto oportunista.*

1. Introdução

Redes oportunistas são redes formadas por dispositivos que possuem mobilidade tamanha que, durante a maior parte do tempo, os nós estão desconectados e se aproveitam de oportunidades de transmissão para encaminhar os dados para outro nó [PELUSI et al. 2006]. Tais oportunidades acontecem quando os nós, através do deslocamento dos seus portadores, entram no alcance do rádio de outro dispositivo e podem se comunicar. De oportunidade em oportunidade, os dados vão sendo transferidos de nó para nó até que alcance o destinatário. Essas mensagens que são encaminhadas pela rede, em geral, são oriundas das aplicações.

Nas redes oportunistas, algumas aplicações propostas são de utilização para busca e salvamento nos chamados cenários de emergência, onde toda ou parte da infraestrutura de comunicação é atingida e danificada por eventos que isolam uma

determinada região. Ou ainda, em cenários onde a Internet não está disponível para determinados nós, funcionando como uma rede de acesso destes nós para a Internet, por exemplo. É provável que o motivo de existirem aplicações desse tipo se deve ao fato de que o conjunto de conhecimento sobre redes oportunistas não permite ainda, a execução de aplicativos diversos com o mesmo desempenho, quando comparados aos similares executados em redes cabeadas ou redes móveis das companhias telefônicas. Embora, originalmente, os principais fatores impulsionadores da pesquisa em redes oportunistas fossem os ditos cenários de emergência e levar conectividade a regiões rurais e sem infraestrutura, outros cenários parecem surgir como possíveis locais onde redes oportunistas poderiam ser usadas. Locais esses que, mesmo com a presença de redes sem fio infraestruturadas ou cobertura 3G/4G, não tem requisitos como liberdade de expressão ou baixo custo de acesso a Internet.

Dentro deste contexto, o presente trabalho tem como objetivo discutir os desafios relacionados à troca de arquivos nas redes oportunistas. Com base nesses desafios é proposta uma aplicação para troca de arquivos usando o paradigma P2P nessas redes, de maneira independente a qualquer tipo de infraestrutura e possuindo as características adequadas para o ambiente oportunista. Assim, a aplicação proposta foi avaliada via simulação sobre diferentes protocolos de roteamento oportunistas. Como contribuição do presente artigo, a aplicação proposta busca reduzir o tempo de resposta da comunicação ao permitir que nós intermediários possam contribuir na disseminação dos arquivos e isso é mostrado através dos resultados obtidos em um cenário simulado.

2. Trabalhos relacionados

Em [YANG et al 2006] é apresentado um esquema de persistência, busca e recuperação de arquivos utilizando o particionamento de arquivo para melhorar as transferências. São selecionados nós com grande espaço de armazenamento para guardar as mensagens quando ocorrer erro em uma transferência. Quando a conectividade for reestabelecida, o arquivo é recuperado a partir desses nós. A pré-configuração dos nós é um ponto crítico para a proposta, pois, além de selecionar os nós que funcionarão provendo o serviço de armazenamento, também é necessário que todos os nós conheçam o endereço de todos os demais nós existentes na rede. Esses dois requisitos aliado a presunção de rotas fim-a-fim em redes oportunistas/DTN parece reduzir bastante o cenário de atuação dessa solução. Outro fator limitante, é que necessita para uma melhor performance da existência de nós estáticos. Não faz qualquer menção ao tamanho máximo do arquivo que esse sistema poderia suportar, nem os requisitos necessários dos dispositivos móveis a serem utilizados.

Em Bluetorrent [JUNG et al. 2007] é proposta uma solução de disseminação de conteúdo através da implementação do protocolo Bittorrent em ambiente móvel com o protocolo Bluetooth. Assim como Bittorent, Bluetorrent mantém registros de bons nós por um determinado tempo para favorecê-los em outra oportunidade, mas a escolha de bons nós é realizada em parâmetros opostos. Enquanto [JUNG, S. et al. 2007] pretere os nós com maior duração de conexão, Bittorrent procura mantê-los. Não fica claro no trabalho se de alguma forma conseguiram modificar a implementação do Bluetooth para conseguir realizar inquiry e conectar a outros nós ao mesmo tempo, pois para realizar o inquiry, o dispositivo precisa estar em Inquiry State o que não permite outras operações. Além disso, não fica claro se todas as mensagens do Bittorrent foram implementadas, pois as estratégias de choke/unchoke e interested/not interested não seriam interessantes em um ambiente oportunístico.

Um sistema de distribuição de podcasts é proposto em [LENDERS et al 2007] utilizando Bluetooth para disseminação dos canais de informação. O conteúdo é obtido da Internet através de pontos de acesso instalados ao longo da área. Uma vez que um nó consiga recuperar o podcast, passa a distribuí-lo aos solicitantes.

Outro trabalho que se utiliza de uma estratégia mista com nós fixos é o R-P2P [DE PELLEGRINI et al 2008]. A arquitetura proposta usa três tipos de dispositivos de comunicação: throwboxes, nós usuários e fontes. Os throwboxes formam uma rede IP estática com grande capacidade de armazenamento com o intuito de disseminar e manter os dados disponíveis. Possuem uma segunda interface que permite a comunicação com os nós usuários. Quando um usuário transfere o conteúdo para um throwbox, deleta de seu sistema de arquivos local.

Um modelo que usa nós estáticos móveis é descrito em [WANG et al. 2013] sobre os padrões de movimentação dos nós em um cenário realístico. Com esse modelo, um protocolo de encaminhamento de mensagens é criado para prover uma rede P2P que não dependa de um serviço ou infraestrutura. Entretanto, o trabalho não detalha as características dos dispositivos nem de que tipo de arquivos ou tamanhos dos mesmos seria suportado. Faltam também maiores informações sobre a camada de aplicação.

Em [HELGASON et al 2010] é apresentada uma proposta de um middleware que não necessita de infraestrutura para prover serviços a camada de aplicação. Como outras propostas, uma classificação de conteúdo é criada para organizar as entradas e facilitar a busca. Embora o cenário de atuação seja redes oportunistas a validação consistiu em um conjunto de nós fixos.

Em [MCNAMARA et al 2008], uma aplicação é proposta para troca de arquivos de músicas entre usuários do metrô de Londres usando Bluetooth. Esse trabalho explora um sistema de categorização de conteúdo através das tags e meta informações de arquivos de música obtidos a partir das listas de execução dos usuários do sistema. Os dados utilizados são de usuários de duas linhas do metrô de Londres onde foi introduzido o sistema de pagamento através de cartões com RFID. Os cartões são utilizados para entrar e sair das estações. Assim, o tempo de permanência do usuário no sistema pode ser determinado, faltando estimar se os usuários estão em contato ou não dentro do sistema. Entretanto, os autores não levam em consideração as diferenças da movimentação dos usuários.

Em [GUIMARÃES et al 2013] é abordado o impacto da dinâmica na modelagem de sistemas reais. Assim, os valores do tempo de difusão da informação na rede não correspondem à realidade quando preditos sem levar em conta a dinamicidade do sistema. Além disso, é verificado o ganho de se considerar métricas topológicas dinâmicas para acelerar o processo de difusão de informação nestes sistemas.

3. Problemas relacionados às aplicações de troca de arquivos em redes oportunistas

Como descrito acima, existem muitas propostas para prover troca de arquivos em redes ad hoc. Contudo, há algumas decisões nos trabalhos que levam a questionamentos sobre as propostas e as quão efetivas são. Considerando o objetivo do presente trabalho em verificar a viabilidade de uma solução de troca de arquivos em redes oportunistas, e utilizando a capacidade atual dos smartphones, faz-se necessário: (i) não escolher cenários irreais, (ii) não propor soluções ou técnicas que não sejam triviais de implementar em redes oportunistas, (iii) não se valer de qualquer tipo de dispositivo fixo especial que

possa facilitar os contatos ou manter as mensagens e (iv) não ignorar que as aplicações precisam ser repensadas para funcionarem no contexto oportunístico. Dos trabalhos da seção anterior, podemos classificá-los na Tabela 1 conforme essas observações.

Em relação aos trabalhos que foram classificadas com os itens 1 e 5 da Tabela 1, é entendido que são características dos próprios trabalhos apresentados e, assim, não se enquadram nos objetivos perseguidos no presente trabalho. Quanto aos classificados os itens 2 e 4, é possível que o trabalho estivesse em um momento de transição do conhecimento da área ou da tecnologia no momento de desenvolvimento e hoje pareça não razoável os conceitos aplicados. Assim, como nas simulações realizadas no início da pesquisa da área, o movimento dos nós era feito através do modelo de mobilidade Random Waypoint. Desde então, adquiriu-se maturidade para perceber que isso era inadequado para validar os trabalhos e outros conceitos podem também ter sido tentados dentro do contexto de redes oportunistas, mas não conseguiram se solidificar e prosperar. Trataremos do caso das propostas que não adaptaram os aplicativos para a realidade oportunista ou não exploraram a camada de aplicação com novas estratégias.

#	Observação	Descrição	Trabalhos
1	Aplicações para redes MANET	Trabalhos que se baseiam na premissa de conexão fim-a-fim.	[YANG et al 2006]
2	Suposições muito restritivas no cenário oportunista.	Operações complexas de serem realizadas no contexto oportunístico. Por exemplo, ter conhecimento sobre todos os dispositivos existentes.	[YANG et al 2006], [JUNG et al 2007], [HELGASON et al 2010], [MCNAMARA et al 2008]
3	Falta de importância da camada de aplicação ou não adequação do aplicativo	Ignorar a importância da camada de aplicação ou não adaptar os aplicativos ao contexto oportunista.	[YANG et al 2006], [LENDERS et al 2007], [DE PELLEGRINI et al 2008], [HELGASON et al 2010], [MCNAMARA et al 2008],[WANG2013]
4	Cenários irreais ou com parâmetros exagerados	Utilizar premissas como nós parados, movimento aleatório, tamanho pequeno de cenários ou alcance do rádio exagerado.	[JUNG et al. 2007], [LENDERS et al 2007], [HELGASON et al 2010]
5	Dependência de infraestrutura	Utilizar de qualquer infraestrutura (redes, throwboxes, sistemas externos, etc) para melhorar a troca de mensagens ou fomentar encontros.	[LENDERS et al 2007], [DE PELLEGRINI et al 2008], [WANG et al. 2013]

Tabela 1 - Classificação dos trabalhos de acordo com a não aderência aos objetivos propostos.

3.1. Representação não realista da camada de aplicação

Uma maneira de tornar redes ad hoc multi-salto uma realidade é eliminar a presunção de ser uma rede de propósito geral, criar redes e aplicações especializadas. A grande mobilidade dos nós no contexto oportunista faz com que seja desafiador a transmissão de dados com vários saltos. Estratégias e otimizações têm sido criadas e testadas com o intuito de mitigar a falta de conectividade ocasionada pelo deslocamento entre os nós e melhorar o desempenho de aplicações em um cenário com muitas restrições como, por exemplo, a carga de energia disponível em dispositivos móveis como smartphones.

Dentre as otimizações, há uma mudança de visão de como pensar soluções para redes oportunistas com a estratégia de desenvolvimento orientado às aplicações. Em [CONTI, GIORDANO 2014] são analisadas as necessidades das aplicações antes da construção dos demais componentes, justamente para que as soluções técnicas possam atender aos requisitos. Assim, é inevitável que ao se pensar em uma solução para troca de arquivos em redes oportunistas, leve em consideração as estratégias que possam ser empregadas na camada de aplicação para melhorar a taxa de sucesso. Em muitos

trabalhos, as aplicações são meros geradores de tráfego. Não se preocupar com a camada de aplicação não é um erro, mas é desprezar um conjunto de possibilidades para se alcançar sucesso na implementação de aplicações em redes oportunistas.

3.2. Informação da localização do conteúdo

Em geral, quando é necessário realizar uma pesquisa ou recuperar algum conteúdo, os usuários procuram usar um sistema de busca de informação onde um conjunto de palavras-chave vão retornar localizações do conteúdo pretendido através de algum mapeamento entre termos buscados e o conteúdo. Esse modelo é muito utilizado na Web através dos motores de busca e funciona em cenários onde a conectividade com o sistema de busca e do cliente com o local do conteúdo são presumidas. Nada adianta localizar a fonte se não for possível recuperar o conteúdo. Assim, sistemas de busca com servidores centralizados no contexto oportunista tem a eficácia reduzida em função da falta de disponibilidade do serviço em razão da falta de conectividade. Existem propostas de sistemas de busca distribuídas, mas o esforço para manter mapeamento de palavras-chave entre os nós é tão grande quanto o de manter a topologia de rede. Esses mecanismos criam uma estrutura com as informações de localização do conteúdo entre os nós e, por isso, são chamados de estruturados.

No contexto do presente trabalho, a informação de quem tem partes do arquivo deve ser recuperada para que as chances de obtenção aumentem ao se criar requisições em paralelo a mais de um semeador. O Bittorrent mantém uma estrutura para que todos saibam o IP dos nós participantes do enxame. Assim que um nó obtém uma parte do conteúdo, ele será sinalizado dentro do enxame como detentor de partes do arquivo passando a receber requisições desse conteúdo. Com a proposta de introduzir duas mensagens na comunicação entre os nós desse trabalho, é possível fazer com que os usuários do enxame possam receber as requisições e contribuir devolvendo o conteúdo solicitado caso possuam ou encaminhando a mensagem até alcançar quem tenha.

3.3. Como aproximar o conteúdo do usuário em redes oportunistas

No cenário oportunista, o tempo de transmissão depende da duração dos contatos entre dois nós e que varia de acordo com a movimentação dos nós. Assim, ele é tão duradouro quanto o tempo que as pessoas permanecem juntas (em contato). Isso significa que existe um limite para o número de bytes que podem ser transferidos durante um contato. Se usarmos uma estratégia que permita uma transferência de arquivos de tamanho arbitrário, temos que considerar a possibilidade de transferir a quantidade de bytes possível em um contato e recuperar o restante em outra oportunidade. Mas será possível contar com outra oportunidade no contexto oportunista? Ou com que frequência os nós se reencontram?

Assim, para não depender da popularidade do conteúdo para conseguir que o mecanismo funcione a contento, podem-se empregar alguns princípios oriundos de Redes de Distribuição de Conteúdo (Content Delivery Network – CDN). Uma CDN é um conjunto de servidores distribuídos e interconectados que cooperam para melhorar a experiência do usuário na distribuição de conteúdo. As suas duas principais técnicas são: replicar conteúdo em algum ponto da rede que seja mais próximo do usuário; e redirecioná-lo para este novo servidor. Assim, iremos utilizar do conceito aplicado em CDNs para favorecer o retorno de partes do arquivo. Como exposto em [CHOO et al. 2011], é vantajoso que os nós da rede conheçam a semântica da aplicação para melhorar

o desempenho e que aplicativos de troca de arquivo só possam considerar a transferência bem sucedida se todas as partes do arquivo forem corretamente recebidas.

3.4. Disseminação rápida do conteúdo

Como dito anteriormente, é importante aproximar o conteúdo do usuário para que se possa completar o arquivo mais rapidamente. Assim, é muito importante melhorar a distribuição do arquivo na rede. Dentro desse contexto, podem-se usar os nós intermediários para oferecer partes do arquivo ao invés da solicitação percorrer um caminho mais longo até chegar ao semeador e conseguir maior número de encontros onde existam partes do arquivo que se deseja transferir.

4. Aplicação proposta

A aplicação proposta é denominada ApTA (Aplicação para Troca de Arquivos) e é baseada no Bittorrent. Ela utiliza as características de distribuição de arquivos segmentada em blocos ou em partes, de maneira descentralizada. Essa estratégia permite a entrega de partes do arquivo durante os curtos encontros entre nós em movimento, aumentando a oferta de parte ou bloco dentro do enxame. Nem todas as características do Bittorrent são reproduzíveis ou mesmo desejáveis no cenário sem fio e oportunista, pois as estratégias praticadas no Bittorrent como *tit-for-tat* só funcionam em contextos com conexão de longa duração, algo imprevisível em redes oportunísticas.

4.1. Funcionamento básico da aplicação

Uma vez iniciada a requisição do arquivo, a aplicação irá gerar pacotes de requisição de partes do arquivo a todos os semeadores conhecidos. Em cada requisição, existe o identificador do arquivo que se deseja obter e o número do bloco desejado. Se o nó não possuir nenhum bloco do arquivo, irá enviar uma mensagem de requisição RQP (Requisição de Qualquer Parte). Tais mensagens não especificam uma parte do arquivo e permitem que o nó envie qualquer parte que ele possua. Caso contrário, irá selecionar aleatoriamente um dos blocos faltantes para reiniciar o processo. Cada vez que um nó é encontrado, é verificado se mensagens devem ser trocadas. Caso ocorra uma troca de mensagens e a mesma seja uma requisição, o nó receptor irá procurar no cabeçalho pelo identificador do arquivo e pelo bloco solicitado. Caso possua essa parte do arquivo, ele mesmo irá responder à solicitação devolvendo o bloco e não repassando a mensagem.

4.2. Particionamento dos arquivos

A ideia de dividir o arquivo em blocos menores é a implementação da velha estratégia da computação de dividir para conquistar. Ao invés de tentar transferir todo o arquivo de uma vez como é feito normalmente no protocolo HTTP, em P2P a ideia é incrementar aos poucos o arquivo, recebendo partes do mesmo. Embora seja possível realizar downloads incrementais sobre HTTP através do header Range, não permitiria o mesmo efeito. No Bittorrent, o particionamento é feito para melhorar a escalabilidade e não onerar o nó detentor do arquivo. Quando um nó adquire um bloco de um arquivo, ele passa a servi-lo, criando redundância e escalando a aplicação, pois a cada novo cliente que entre no enxame a procura do arquivo, ele também oferecerá blocos do arquivo já recebidos enquanto estiver a procura dos demais. Essa característica do Bittorrent faz com que a aplicação escale independente do número de nós no enxame. No cenário oportunista, isso não só permitirá a desoneração dos nós inicialmente

detentores do arquivo, como também a oferta de processamento e largura de banda já que todo nó que esteja executando a aplicação irá transportar as mensagens recebidas. Além disso, em cenários onde o tempo de contato entre os nós for pequeno, a estratégia de dividir o arquivo em partes menores parece acertada, pois permitiria a transferência do arquivo aos poucos, aproveitando o pouco tempo de transmissão durante os contatos. O particionamento do arquivo é realizado através de uma divisão lógica do tamanho do arquivo em bytes pelo tamanho em bytes do bloco. Todos os blocos terão o mesmo tamanho, salvo o último que poderá ter tamanho diferente variando entre 1 e N bytes.

4.3. Inicialização de Arquivos

Para começar a recuperar partes do arquivo é necessário saber o endereço dos nós que estejam semeando esse arquivo. Um sistema de pesquisa de arquivos é um tema que está fora dos objetivos do presente trabalho. Existem soluções propostas que poderiam ser implementadas de forma que o usuário final conseguisse realizar pesquisas por nome, tipo de arquivo ou descritores de forma a conseguir a informação necessária para conseguir requisitar o arquivo. Uma forma simples de fazer isso seria armazenar informações sobre os arquivos compartilhados de forma a poder catalogá-lo. O usuário criaria regras através da combinação dessas informações para que a aplicação decidisse se deve ou não iniciar a transferência de um arquivo de acordo com essas regras. As informações dos arquivos de cada nó são trocadas de forma epidêmica a cada encontro. Se as informações de algum arquivo retornado em um encontro forem adequadas de acordo com as regras estabelecidas pelo usuário previamente, a aplicação iniciaria a transferência. De uma forma mais refinada, poderia ser utilizado um esquema de subscrição como proposto em [EUGSTER 2003]. Outra forma interessante seria a impressão de uma imagem contendo um código QR que armazenaria as informações do identificador do arquivo e endereço do nó que publicou e que seriam lidos através das câmeras dos smartphones. Inicialmente, as informações necessárias para o início da aplicação são o endereço do nó original e o número de partes do arquivo. Com o passar do tempo, à medida que está obtendo o arquivo, aplicação vai tomando conhecimento de outros nós para solicitar partes do arquivo.

4.4. Tipos de Mensagens utilizadas

A aplicação utiliza de mensagens de requisição para solicitar partes e mensagens de resposta para devolver a parte solicitada. Como já mencionado, ApTA se utiliza das mensagens RQP para solicitar uma parte qualquer do arquivo o que favorece o recebimento e RespNNS que serão abordadas a seguir. As mensagens usadas pela aplicação possuem um cabeçalho de 3 campos como verificado na Tabela 2.

As mensagens de requisição da aplicação têm em seu cabeçalho os valores de identificação do arquivo e da parte que se deseja obter. Em cenários onde o número de semeadores é muito pequeno em relação ao número total de nós é desejável que partes do arquivo sejam disseminadas rapidamente para que mais fontes dessas partes estejam disponíveis ao longo do enxame, diminuindo o tempo de obtenção da parte solicitada por um nó. O protocolo Bittorrent tem a mensagem HAVE para indicar qual(s) parte(s) de um arquivo um nó já possui. Com isso, o nó anuncia essas partes para outro nó poder solicitar. No cenário oportunista, criar tais mensagens não seria interessante, pois com as grandes latências características dessas redes, provavelmente isso não vai contribuir com a diminuição do tempo de resposta que é o objetivo. Assim, introduzimos as

mensagens Requisição de Qualquer Parte (RQP) para permitir que os nós iniciantes possam adquirir partes mais rapidamente e possam também contribuir com os outros nós oferecendo à rede redundância na oferta dessa parte. Para tal, assumimos o valor especial 5 no campo de identificação da parte do arquivo no cabeçalho da mensagem de requisição. Se o próximo nó que receber essa mensagem tiver alguma parte do arquivo solicitado, ele pode devolver alguma parte selecionada aleatoriamente e impedir que a requisição original continue a se propagar pela rede. O número de vezes que um nó envia mensagens RQP antes de solicitar a parte desejada é parametrizado na aplicação.

Nome	Descrição	Tamanho
Arquivo	Identificador do arquivo solicitado	16 bytes
Parte	Identificador da parte solicitada do arquivo	4 bytes
Tipo	Tipo de mensagem.	1 byte

Tabela 2 - Detalhamento dos campos do cabeçalho das mensagens.

Quanto ao campo "Tipo", os valores possíveis correspondentes aos tipos de mensagem são exibidos na Tabela 3.

Tipo de Mensagem	Request	Response	RQP	RespNNS
Valor	0	1	2	3

Tabela 3 - Valores representativos dos tipos de mensagem

As mensagens Resposta de Nó Não Semeador (RespNNS) servem para os nós intermediários responderem às solicitações por partes do arquivo caso tenham a parte do arquivo solicitada ou a requisição seja uma mensagem RQP e possuam ao menos uma parte do arquivo solicitado. Além disso, esse tipo de mensagem também serve para anunciar que o nó que a enviou faz parte do enxame daquele arquivo. Essa é uma forma sem custo de receber informações sobre os nós participantes.

4.5. Fluxo de ações

Na Figura 1, podemos ver as atividades desempenhadas pelos nós em um ciclo de requisição e resposta.

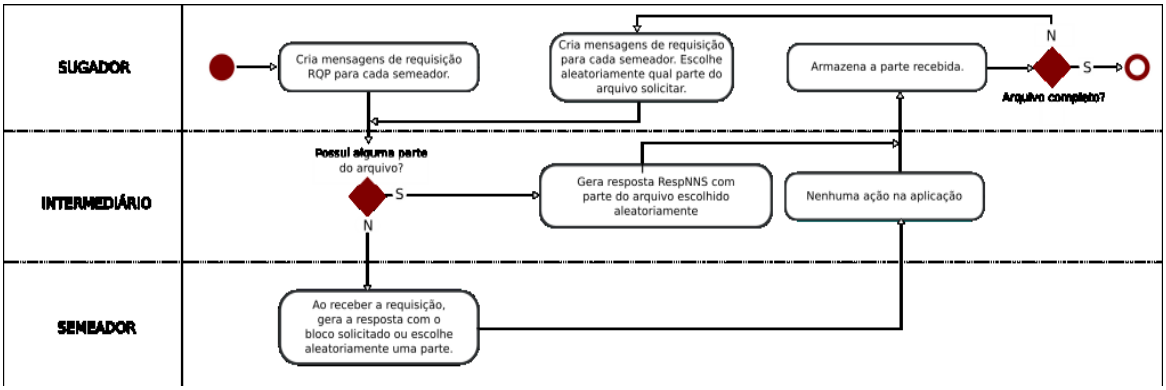


Figura 1 - Fluxo de ações para cada tipo de nó usando APTA.

4.6. Implementação da aplicação ApTA

A aplicação do presente trabalho foi implementada no simulador ONE (Opportunistic

Network Environment) através da classe ApTAApplication estendendo a classe abstrata Application do próprio framework do simulador. Ao iniciar, a aplicação com o auxílio da classe P2PConfig lê suas configurações e verifica se há algum arquivo configurado para ser obtido. Caso exista, ela cria uma requisição RQP para cada um dos semeadores conhecidos. Caso ela possua a cópia completa do arquivo configurado, ela passará a atuar como semeadora e ficará esperando requisições de outros nós.

4.7. Protocolo de encaminhamento baseado em vizinhos no local

Com o intuito de mostrar que a análise das métricas de rede não garante que uma aplicação vá ter bom desempenho em uma rede oportunista, propomos um protocolo denominado LocalScan que é baseado no algoritmo depth-width-search. O algoritmo depth-width-search faz parte de um protocolo proposto no mesmo trabalho onde o cenário é dividido em zonas e a cada encontro tenta-se enviar a mensagem para as zonas frequentadas pelo destinatário através da análise das zonas frequentadas pelos nós durante o encontro. Tal protocolo será referenciado daqui em diante com o nome de DepthWidthSearch. Quando os nós se encontram, eles trocam as informações de zonas frequentadas e cada nó avalia se deve ou não repassar alguma mensagem com base nessa informação e nas zonas dos destinatários das mensagens.

Ao invés de dividirmos o cenário em zonas, iremos mapeá-lo através da percepção dos nós à volta. De tempos em tempos, os nós enviarão beacons de sinalização a procura de nós a volta. Isso já é uma prática no mundo oportunista, pois é preciso detectar nós para se ter encontros. De acordo com a resposta, o nó cria uma entrada com uma lista de representações do endereço MAC dos nós que responderam. Essa lista de representações dos endereços MAC dos nós se chama lista de grupos de contatos. Se um registro de contato for um subconjunto de outro registro de contato, o menor registro será removido dos registros. Esse processo criará um mapeamento espaço-temporal dos nós encontrados. Essa informação será usada para que os nós encaminhem as mensagens apenas aos nós que tiveram contato direto com os nós destinatários das mensagens sendo, portanto, um protocolo de disseminação controlada.

Quando ocorre um encontro, os nós trocam as suas listas de grupos de contatos. Cada nó verifica se carrega alguma mensagem para ser entregue ou repassado ao nó encontrado. Para verificar a possibilidade de repassar alguma mensagem ao nó encontrado, o nó verifica a própria lista de grupos de contatos e a lista de grupos de contatos trocada durante o encontro. Se algum grupo da lista contiver o endereço MAC do nó encontrado e do nó destinatário da mensagem, o nó deverá repassar cópia da mensagem para o nó encontrado com o intuito de melhorar as chances de entrega da mensagem. A ideia é verificar se os nós tiveram em contato e, com essa informação, decidir se a mensagem deve ser repassada ou não para um nó que tenha probabilidade de reencontro com o destinatário da mensagem.

5. Avaliação de desempenho realizada

Nesta seção apresentaremos a avaliação realizada na aplicação ApTA através da descrição dos traces reais utilizados, o cenário de simulação e os resultados obtidos.

5.1. Traces reais de movimento

Para o presente trabalho, foi utilizado o dataset da rede do campus da Universidade de Dartmouth. A coleta de dados nas redes locais sem fio de Dartmouth que compõem esse

dataset começou em abril de 2001 e persistiu até outubro de 2006. O dataset tem as informações de timestamp, nome do ponto de acesso, endereço MAC da estação e tipo de mensagem. O período do dataset usado no presente trabalho foi o compreendido entre 21 de setembro e 20 de outubro de 2003. Esse período foi escolhido em função de ausência de falhas na captura de dados, o que acontece em alguns períodos. Foram escolhidos 100 nós dos 7602 existentes no dataset que tivessem mais registros dentro do período escolhido. Outro critério de escolha foi o número de pontos de acesso visitados no intervalo de tempo. Como existem desktops que se conectam a rede sem fio da universidade, foi usado o limite mínimo de 10 pontos de acesso visitados para ser selecionado. A razão dessa decisão está em usar apenas nós móveis.

Para realizar a simulação, foi utilizado o simulador ONE. Para o presente trabalho, foram implementados os mecanismos DepthWidthSearch e LocalScan. Foram implementados dois relatórios para poder extrair as métricas que permitiram validar a presente proposta. O ReportTime é um relatório implementado através de um *listener* de aplicação. As aplicações ApTA e P2PSimples registraram os eventos abaixo, com exceção dos eventos P2PMSG_HAVE_SENT e P2PMSG_DUPLICADO que são exclusivos da aplicação ApTA. Também foi implementada a aplicação P2PSimples que é uma aplicação geradora de tráfego simples que servirá de comparação. Para não ser tendencioso, não foram implementados mecanismos como os algoritmos *rarest first*, nem o jogo *tit-for-tat* na aplicação P2PSimples, pois entendemos que esses mecanismos funcionam bem em um contexto onde a conectividade pode ser presumida, o que não é o caso das redes oportunistas.

As duas aplicações têm em comum o funcionamento inicial. Ao iniciar, as aplicações geram uma mensagem de requisição de parte do arquivo para cada um dos semeadores de acordo com o número de semeadores parametrizado. A cada requisição recebida, o semeador envia uma resposta. Ao receber a resposta, o sugador envia nova requisição solicitando uma nova parte e esse processo continua até que o arquivo se completa. A diferença entre as duas implementações reside em dois pontos: (i) - Na requisição inicial, a aplicação ApTA envia uma mensagem de requisição RQP cujo valor da identificação do bloco é 5 para cada um dos semeadores conhecidos. A aplicação P2PSimples sorteia aleatoriamente o número do bloco a ser solicitado dentre os que o nó ainda precisa obter. (ii) - Quando um nó que não é a origem nem o destino da mensagem, chamado de nó intermediário recebe uma requisição, ele verifica se possui o bloco do arquivo solicitado. Se possuir, ele devolve o bloco através de uma mensagem de resposta RespNNS. Na aplicação P2PSimples, não há qualquer ação por parte do nó intermediário nesse caso.

A Figura 2 descreve o fluxo de ações para o tratamento de mensagens de acordo com o nó que recebe a requisição na aplicação P2PSimples.

5.2. Cenário de Simulação

A simulação foi realizada com os traces descritos na Seção 5.1 e foram escolhidos os seguintes protocolos de roteamento de redes oportunistas: Spray and Wait, BUBBLE Rap, MaxProp, ProPHET [CHAKCHOUK 2015], DepthWidthSearch [WANG et al 2013]. Esses protocolos foram escolhidos por explorarem diferentes propriedades da mobilidade humana (espacial, temporal e social). Além disso, permitir avaliar a diferença entre essas abordagens de roteamento em relação ao comportamento da rede e às aplicações implementadas (ApTA e P2PSimples) no presente trabalho.

Todos os parâmetros tiveram valores default de implementação. Essa decisão foi

necessária porque os trabalhos referentes aos protocolos escolhidos exploram valores diferentes para os parâmetros para analisar a influência dos mesmos no comportamento da rede. Como simular cada um dos muitos parâmetros e suas possibilidades exigiria um esforço que suplantaria o disponível para este trabalho, decidimos optar por valores definidos na literatura e que não fossem tendenciosos em uma das métricas usadas para avaliar o comportamento de rede. As implementações do Spray and Wait, ProPHET e MaxProp são as implementações fornecidas juntamente com o simulador ONE. A implementação do BUBBLE Rap foi desenvolvida por P.J. Dillon da Universidade de Pittsburgh e foram utilizados valores default para os parâmetros dos protocolos.

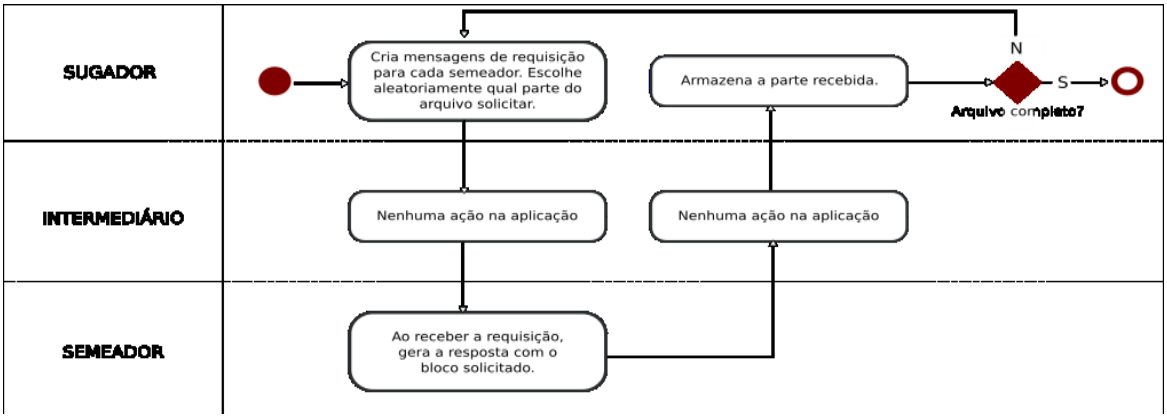


Figura 2 - Fluxo de ações para cada tipo de nó usando P2PSimples

Foram configurados diferentes números de semeadores (1, 5, 10 e 20 escolhidos aleatoriamente) para observar a disseminação de conteúdo. O tamanho dos arquivos utilizados foi de 512KB que representaria uma foto tirada com uma câmera de um celular, por exemplo, ou documento em texto de dezenas de páginas. Foi adotado o padrão 802.11b em modo ad hoc a taxa de 11 Mbps e alcance dos rádios de 50 m. As mensagens usadas pelas aplicações têm tamanho de 21 bytes para requisições, 21 bytes de cabeçalho e 64 KB de dados para as respostas, totalizando 65.557 bytes. O tamanho do buffer dos nós foi configurado para 100MB e o TTL das mensagens foi configurado igual ao tempo total de simulação (864.000 segundos que equivale a 10 dias).

Para avaliar o comportamento das aplicações P2P Simples e ApTA e verificar se os mecanismos de roteamento usados lograram êxito em aproximar o conteúdo do usuário e acelerar a disseminação das partes do arquivo no enxame, foi usada a métrica **número de nós com cópia completa** que é o número de nós que conseguiram reunir todas as partes do arquivo solicitado.Para avaliar o impacto na rede, foi avaliado o **atraso médio** para a entrega das mensagens.

5.3. Resultados obtidos

Muitos trabalhos tentam contribuir com aplicações para o cenário oportunista, persistindo na ideia de que uma rede oportunista seja uma rede de uso geral. Então, realizam experimentos baseados no encaminhamento de mensagens em rede, argumentando terem conseguido entregar mais mensagens, com menor custo, no menor tempo. Mas será que isso é o suficiente para que uma aplicação de troca de arquivos no contexto oportunista tenha sucesso?

Assim, a métrica que iremos analisar é o número de nós sugadores que conseguem reunir todas as partes do arquivo e possuem ao final do tempo do

experimento uma cópia completa do arquivo em seu buffer. Analisando a Figura 3(a), vemos que todos os protocolos tiveram comportamento parecido. Ao longo do tempo de simulação que compreendeu 10 dias, ao menos 8% dos nós conseguiram completar o arquivo com apenas 1 nó fazendo o papel de semeador. Como vimos nas métricas anteriores, o ProPHET replica mais mensagens durante o seu funcionamento e consegue uma pequena vantagem em relação aos outros protocolos, salvo o MaxProp que o acompanha conseguindo os mesmos resultados. À medida que o número de semeadores aumenta e, por consequência, o número de mensagens também aumenta e o número de nós que conseguiram completar o arquivo vai diminuindo devido a congestionamentos e utilização maior do buffer. Observando a Figura 3(c), vemos que apenas o MaxProp consegue entregar partes do arquivo o suficiente para completar alguns poucos usuários.

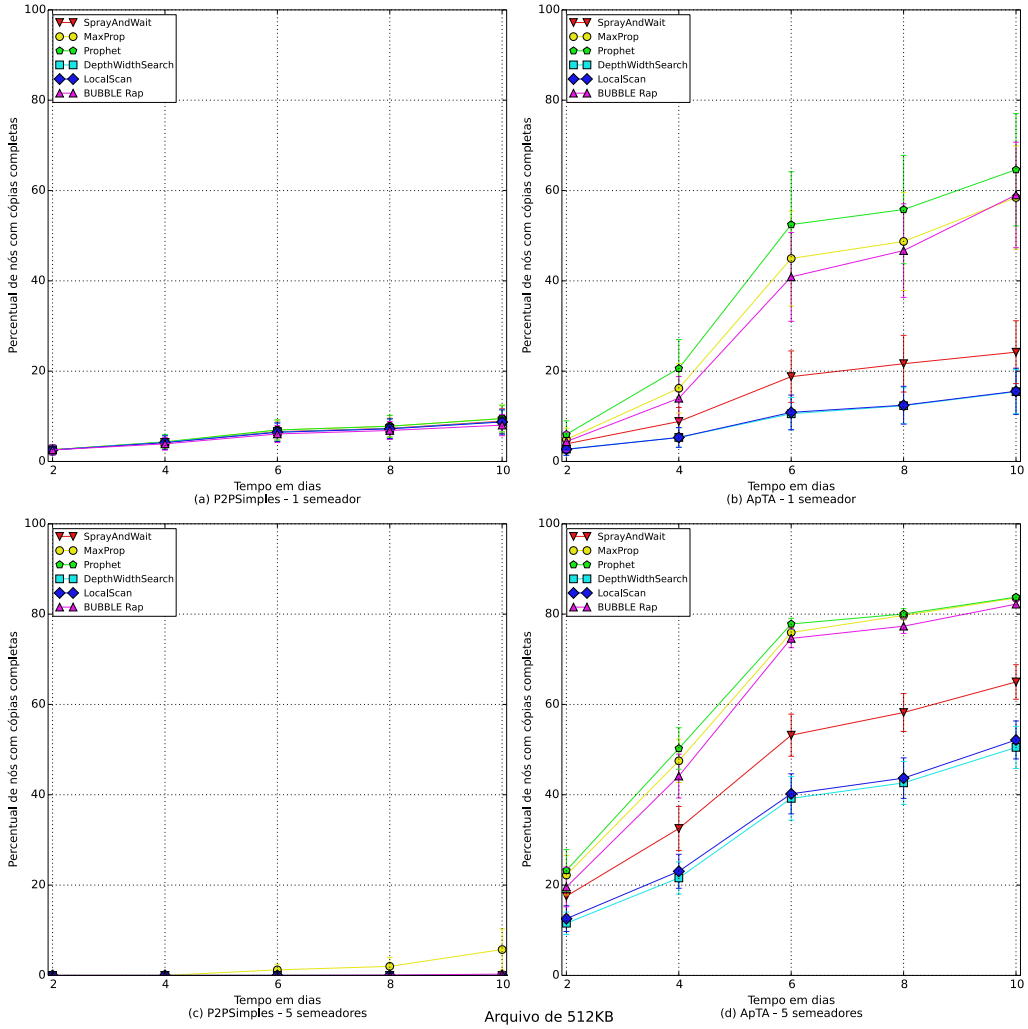


Figura 3 - Percentual de nós com cópias completas com arquivo de 512KB para 1 e 5 semeadores usando as aplicações P2PSimples e ApTA.

Quanto à aplicação ApTA, as Figuras 3(b) e 3(d) mostram de imediato que os resultados foram muito melhores que na aplicação P2PSimples. Em aproximadamente 3 dias, a aplicação ApTA consegue distribuir o arquivo de 512K com 1 semeador para o mesmo número de nós que a aplicação P2PSimples em todo o período de simulação. Ao final da simulação, usando o protocolo de encaminhamento ProPHET,

aproximadamente 65% dos usuários conseguiram completar o arquivo com apenas 1 semeador. Também teve bom desempenho a aplicação ApTA com a utilização dos protocolos BUBBLE Rap e MaxProp com aproximadamente 60% de nós completos. Isso é mais do que 5x o número de nós completos com o uso da aplicação P2PSimples.

Outro ponto importante é que, com o aumento do número de mensagens em função do acréscimo de semeadores, a aplicação ApTA conseguiu que mais nós conseguisse completar o arquivo, ao contrário do que aconteceu com a aplicação P2PSimples, chegando a mais de 80% de nós com cópia completa do arquivo em seus buffers com todos os protocolos de encaminhamento.

Na Figura 4 é mostrado o atraso médio para a entrega das mensagens e percebemos que, em geral, segue a tendência de acompanhar o crescimento do número de semeadores no caso da aplicação P2PSimples. Esse fato se deve, mais uma vez, em grande parte ao aumento do número de mensagens na rede, uma vez que as aplicações solicitavam partes a todos os semeadores. Já utilizando a aplicação ApTA, o atraso se mantém praticamente constante mesmo com o aumento do número de semeadores, pois, a medida que o tempo passa, a distribuição do conteúdo permite que o mesmo seja recuperado a partir de nós mais próximos o que mitiga o atraso. Os protocolos com maior controle de disseminação tiveram menores atrasos da seguinte forma. Spray and Wait, DepthWidthSearch e LocalScan têm comportamentos muito parecidos em função do aumento dos semeadores. Os protocolos BUBBLE Rap, ProPHET e MaxProp tiveram um comportamento parecido e apresentaram maior atraso que os outros três. O LocalScan foi o que apresentou o menor atraso usando a aplicação P2PSimples.

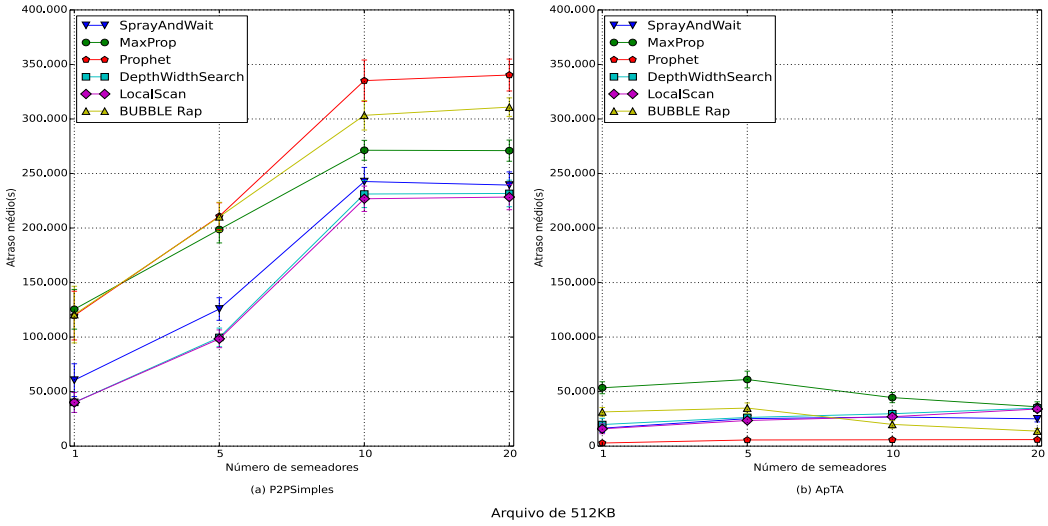


Figura 4 - Atraso médio das duas aplicações variando o roteamento e o número de semeadores.

Já na aplicação ApTA (ver Figura 4(b)), os protocolos Spray and Wait, DepthWidthSearch e LocalScan também apresentaram comportamentos muito parecidos e têm valores de atraso medianos em relação aos demais protocolos. Os protocolos BUBBLE Rap e MaxProp têm o mesmo comportamento com o valor máximo de 5 semeadores. Já o protocolo ProPHET foi o que teve melhor desempenho.

6. Conclusão

Neste artigo apresentamos alguns problemas relacionados a aplicações de troca de arquivos em redes oportunistas como a representação não realística da camada de

aplicação que pode interferir na avaliação de desempenho. Assim, foi proposta a aplicação ApTA para atender a esses requisitos. Na análise de desempenho realizada, verificamos que o trabalho alcançou o objetivo almejado, pois além de mostrar que a aplicação ApTA teve êxito em aproximar o conteúdo do usuário, acelerou a disseminação do conteúdo dentro do enxame e conseguiu aproveitar o acréscimo de nós semeadores, fatos que não foram percebidos na aplicação P2PSimples.

Verificamos uma grande diferença na avaliação de desempenho de trabalhos que usam uma aplicação real e uma aplicação pouco realística (P2PSimples), em que no presente trabalho chamamos de representação vazia da camada de aplicação. É importante avaliar o impacto dessa condição em outros cenários de redes oportunistas.

Referências

[PELUSI et al 2006] PELUSI, ; PASSARELLA, ; CONTI,. Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. IEEE Communications Magazine, v. 44, n. 11, p. 134-141, 2006.

[LINDGREN, HUI 2009] LINDGREN, A.; HUI, P. The quest for a killer app for opportunistic and delay tolerant networks. 4th ACM CHANTS. 2009.

[WANG et al 2013] WANG, S. et al. Opportunistic routing in intermittently connected mobile P2P networks. IEEE Journal on Selected Areas in Communications, v.31, n.9, 2013.

[PASSARELLA 2012] PASSARELLA, A. A survey on content-centric technologies for the current Internet: CDN and P2P solutions. Computer Communications, v. 35, n. 1, 2012.

[YANG et al. 2006] YANG, G. et al. Ad-hoc storage overlay system: A delay-tolerant approach in manets. IEEE MASS, 2006.

[JUNG et al. 2007] JUNG, S. et al. Bluetorrent: Cooperative content sharing for bluetooth users. Pervasive and Mobile Computing, v. 3, n. 6, p. 609-634, 2007.

[LENDERS et al. 2007] LENDERS, V.; KARLSSON , G.; MAY, M. Wireless ad hoc podcasting. 4th IEEE SECON'07, 2007. p. 273-283.

[DE PELLEGRINI , et al 2008] DE PELLEGRINI , F. et al. R-P2P: a data centric DTN middleware with interconnected throwboxes. 2nd ICST. 2008. p. 2.

[HELGASON et al. 2010] HELGASON, Ó. R. et al. A mobile peer-to-peer system for opportunistic content-centric networking. 2nd ACM SIGCOMM Mobiheld. 2010.

[MCNAMARA et al. 2008] MCNAMARA, ; MASCOLO, C.; CAPRA, L. Media sharing based on colocation prediction in urban transport. 14th ACM Mobicom 2008.

[CONTI, GIORDANO 2014] CONTI, M.; GIORDANO, S. Mobile ad hoc networking: milestones, challenges, and new research directions. IEEE Com. Magazine, v.52, n.1, 2014.

[CHOO et al. 2011] CHOO, C.; SESHADRI, P. V.; CHAN , M. C. Application-aware disruption tolerant network. 8th IEEE MASS, 2011.

[EUGSTER 2003] EUGSTER, T. et al. The many faces of publish/subscribe. ACM Computing Surveys, v. 35, n. 2, p. 114-131, 2003.

[CHAKCHOUK 2015] CHAKCHOUK , N.; A survey on opportunistic routing in wireless communication networks, IEEE Communications Surveys & Tutorials, v. 17, no. 4, 2015.

[GUIMARÃES et al. 2013] GUIMARÃES, A. VIEIRA, A., SILVA A., ZIVIANI A. Fast Centrality-Driven Diffusion in Dynamic Networks. ACM WWW 2013.

Realização

Apoio Fomento

Apoio Institucional

Patrocinador Diamante

Núcleo de Informação e Coordenação do Ponto BR

Comitê Gestor da Internet no Brasil

Patrocinador Ouro

Patrocinador Bronze